УНИВЕРСИТЕТ ПРОКУРАТУРЫ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ОБЩЕРОССИЙСКАЯ ОБЩЕСТВЕННАЯ ОРГАНИЗАЦИЯ
«РОССИЙСКАЯ КРИМИНОЛОГИЧЕСКАЯ АССОЦИАЦИЯ»

ЦИФРОВЫЕ ТЕХНОЛОГИИ В БОРЬБЕ С ПРЕСТУПНОСТЬЮ: ПРОБЛЕМЫ, СОСТОЯНИЕ, ТЕНДЕНЦИИ

(Долговские чтения)

Сборник материалов
I Всероссийской научно-практической
конференции

(Москва, 27 января 2021 г.)

Москва ● 2021

УДК 343.85
ББК 67.515
Ц75

Под общей редакцией **О.С. Капинус**, ректора Университета прокуратуры Российской Федерации, доктора юридических наук, профессора.

Научное редактирование:
В.В. Меркурьев, заведующий отделом НИИ Университета прокуратуры Российской Федерации, доктор юридических наук, профессор;
П.В. Агапов, главный научный сотрудник НИИ Университета прокуратуры Российской Федерации, доктор юридических наук, профессор.

Составители:
М.В. Ульянов, ведущий научный сотрудник НИИ Университета прокуратуры Российской Федерации, кандидат юридических наук;
Н.В. Сальников, научный сотрудник НИИ Университета прокуратуры Российской Федерации.

Рецензенты:
А.Г. Залужный, профессор кафедры правового обеспечения национальной безопасности Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации, доктор юридических наук, профессор;
С.В. Расторопов, профессор кафедры Университета прокуратуры Российской Федерации, доктор юридических наук, профессор.

Ц75 **Цифровые технологии в борьбе с преступностью: проблемы, состояние, тенденции (Долговские чтения):** сб. материалов I Всерос. науч.-практ. конф. (Москва, 27 января 2021 г.) / под общ. ред. О.С. Капинус; [науч. ред. В.В. Меркурьев, П.В. Агапов; сост. М.В. Ульянов, Н.В. Сальников]; Ун-т прокуратуры Рос. Федерации. – М., 2021. – 460 с.

В сборник включены выступления и доклады участников I Всероссийской научно-практической конференции «Цифровые технологии в борьбе с преступностью: проблемы, состояние, тенденции (Долговские чтения)», проведенной в Университете прокуратуры Российской Федерации 27 января 2021 г., а также рекомендации, выработанные по итогам обсуждения темы конференции. В работе научного собрания приняли участие научные, педагогические и практические работники Генеральной прокуратуры Российской Федерации, Университета прокуратуры Российской Федерации, Научно-практического центра проблем укрепления законности и правопорядка Генеральной прокуратуры Республики Беларусь, Московской академии Следственного комитета Российской Федерации, ВНИИ МВД России, Московского университета МВД России имени В.Я. Кикотя, иных научных и образовательных организаций.

Для работников прокуратуры, органов судебной власти и правоохранительных органов, научных и педагогических работников, докторантов, аспирантов, магистрантов и студентов, интересующихся проблемами предупреждения преступлений, совершаемых с использованием информационно-телекоммуникационных сетей.

Должности участников конференции указаны на момент проведения мероприятия. Доклады и выступления изложены в авторской редакции.

УДК 343.85
ББК 67.515

© Университет прокуратуры Российской Федерации, 2021
© Российская криминологическая ассоциация, 2021

А.В. Разинкин,
заместитель Генерального прокурора
Российской Федерации

Вступительное слово

Уважаемые коллеги! Стремительное развитие информационных технологий предопределяет вовлечение все большего числа граждан в цифровую среду. Социальные сети, мессенджеры, средства электронных платежей и, конечно же, сама сеть «Интернет», являясь неотъемлемой частью современного человека, становятся при этом все более привлекательными для противоправного поведения.

Распространенность преступлений, совершенных при помощи цифровых технологий, количество которых в 2020 г. превысило полмиллиона (510,3 тыс.), увеличившись на 73,4%, вызывает серьезную обеспокоенность и находится на особом контроле в Генеральной прокуратуре Российской Федерации.

Их основная масса, как правило, совершается с использованием сети «Интернет» (300 тыс.), средств мобильной связи (218 тыс.) и расчетных (пластиковых) карт (190 тыс.).

Почти половина (237 тыс.) таких криминальных посягательств квалифицированы как хищение чужого имущества по ст. 158–159[6] УК РФ. При этом чаще всего для реализации преступного умысла используются методы социальной инженерии.

По-прежнему с использованием сети «Интернет» совершается большое количество наркопреступлений, а также деяний экстремистской и террористической направленности. Все большую актуальность приобретают посягательства, связанные с нарушением неприкосновенности частной жизни, незаконным получением сведений, составляющих коммерческую и иную охраняемую законом тайну, неправомерным оборотом средств платежей, незаконным оборотом оружия и сильнодействующих веществ.

Увеличивается и число посягательств на критическую инфраструктуру. В среднем каждая третья выявляемая атака направлена на организации кредитно-финансовой сферы, при-

мерно столько же – на органы госвласти, десятая часть приходится на социальные объекты и объекты обороны. И хотя все они успешно отражаются, растущее из года в год их количество и использование при их совершении инфраструктуры зарубежных государств обращают на себя пристальное внимание со стороны правоохранительных органов и центров реагирования на компьютерные инциденты.

При этом, к сожалению, по специальным статьям в сфере компьютерной информации, отнесенным к гл. 28 УК РФ, квалифицировано только 4498 преступлений.

Таким образом, более чем остро стоит задача по противодействию киберугрозам и использованию в этих целях тех же информационных технологий для прогнозирования, предупреждения и своевременного устранения недостатков нормативного правового регулирования.

Что касается работы органов правоохраны в данной сфере, эффективность этой деятельности в июле прошлого года рассмотрена на Координационном совещании руководителей правоохранительных органов Российской Федерации. Анализ ключевых проблем показал, что они связаны не только с правоприменительной практикой, но и с правовыми пробелами, устранение которых требует в первую очередь научного подхода. Поэтому по итогам обсуждения помимо совершенствования методов и способов выявления, раскрытия и расследования киберпреступлений предложены мероприятия, направленные и на теоретическую проработку комплекса вопросов.

Прежде всего, это относится к методологическому обеспечению деятельности специализированных киберподразделений правоохранительных органов, которое учитывало бы специфику раскрытия и расследования преступлений в области IT-технологий.

Ведется работа по активизации механизмов государственно-частного партнерства, поскольку ключевое значение для эффективного противодействия рассматриваемым преступлениям имеет качество взаимодействия с организациями, располагающими оперативно значимой информацией. Это банки, операторы связи, интернет-провайдеры, владельцы интернет-сервисов, центры реагирования на компьютерные инциденты и организации сферы кибербезопасности. Вместе с тем во взаимодействии с научным

сообществом еще предстоит проработать механизмы и порядок такой совместной деятельности.

Безусловно, активно совершенствуется и законодательство, которое по мере появления новых вызовов пополняется соответствующими нормами. Это касается расширения признаков преступлений в сфере IT-технологий, актуализации перечня противоправных деяний в киберпространстве, подлежащих криминализации, расширения терминологии. Однако законодательная база должна формироваться значительно быстрее.

К примеру, в 2020 г. введена регламентация оборота цифровых финансовых активов и криптовалюты. Несомненно, разрешение на законодательном уровне основных подходов к урегулированию их оборота позволит более эффективно осуществлять противодействие финансированию преступных групп, терроризма и коррупции. Между тем законодателем так и не определены пределы уголовной ответственности в области оборота криптовалюты, поэтому проблематика введения соответствующих запретов прорабатывается в настоящее время во взаимодействии со всеми заинтересованными структурами.

Немало вопросов и к существующим уголовно-правовым нормам, которые подлежат совершенствованию с учетом современных тенденций и угроз в области информационной безопасности. Это касается основополагающих понятий, используемых в гл. 28 УК РФ, внедрения новых форм уголовно наказуемых деяний, усиления ответственности за преступления в сфере оборота персональных данных или компьютерной информации, а также работы по иным направлениям.

Значительные сложности имеются и в процессуальной деятельности, связанной с собиранием доказательств, фиксацией преступных цифровых следов, последующим хранением и использованием таких доказательств и, самое главное, использованием новых технических возможностей для производства следственных и иных процессуальных действий. Очевидно, что без активного расширения правового регулирования на этом направлении, в том числе выводов и рекомендаций научного сообщества, правоприменителю будет сложно достичь значимых результатов.

Немало вопросов вызывает и уровень международного сотрудничества в сфере противодействия цифровой преступности.

В истекшем году активизирована подготовка проекта всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях и единого глоссария к ней. Для этих целей, в частности, создана межведомственная рабочая группа по противодействию информационной преступности.

Продвижение российских инициатив обеспечивается в том числе в ходе мероприятий, посвященных проблематике борьбы с киберпреступлениями, организованных на площадках Совета Европы, АСЕАН, БРИКС, а также ООН, в частности в рамках работы Группы правительственных экспертов и Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной информационной безопасности.

Вместе с тем большинство обсуждаемых вопросов не урегулировано российским законодательством, носит теоретический характер и нуждается в нормативном толковании.

Уважаемые коллеги, несмотря на наличие определенных механизмов противодействия использованию информационных технологий в противоправных целях, проблем все еще много. Для перелома ситуации важны единообразное понимание стоящих перед нами вызовов и угроз и четко скоординированная работа по их нейтрализации с привлечением научного потенциала. Не сомневаюсь, что высказанные на конференции идеи и инициативы позволят скорректировать дальнейшую работу.

О.С. Капинус,
ректор Университета прокуратуры
Российской Федерации,
доктор юридических наук, профессор

Вступительное слово

Уважаемые участники конференции! Безусловно, поднимаемая нами проблематика использования цифровых технологий в борьбе с преступностью из года в год приобретает все большую актуальность, и тому есть объективные причины. Неслучайно в соответствии с Указом Президента Российской Федерации от 25.12.2020 № 812 в 2021 г. в России проводится Год науки и технологий. Определенные шаги к противодействию преступности законодательными, судебными и правоохранительными органами предпринимаются, и мы не остаемся в этих вопросах сторонними наблюдателями. Мероприятия проводятся в рамках Плана работы Университета прокуратуры Российской Федерации, утверждаемого заместителем Генерального прокурора Российской Федерации.

Следует отметить, что уже традиционно, более десяти лет, проводятся научные форумы, организованные Университетом прокуратуры Российской Федерации совместно с Российской криминологической ассоциацией. Отдавая дань уважения памяти, подчеркну, что президентом Ассоциации долгие годы являлась известный ученый-криминолог, доктор юридических наук, профессор Азалия Ивановна Долгова.

Уверена, что главный способ увековечить память ученого – дать мощный импульс для развития отечественной науки и поддержать молодые таланты, чему в полной мере способствует наша конференция, получившая название «Долговские чтения».

Приятно видеть среди участников ученых, политиков, представителей власти, правоохранительных органов из 23 субъектов Российской Федерации, республик Беларусь и Абхазия.

Активное развитие информационно-коммуникационных технологий наряду с прогрессивными аспектами, о которых мы также поговорим, порождает новые угрозы государственной и общественной безопасности.

Играя ведущую роль в координации деятельности правоохранительных органов по борьбе с преступностью, органы прокуратуры сегодня активно противодействуют преступлениям, совершаемым с использованием современных информационно-коммуникационных технологий.

По мере развития цифровых технологий и способов их незаконного использования совершенствуются и способы выявления цифровых следов преступной деятельности.

Остановлюсь подробнее на некоторых изменениях, которые произошли в мире с развитием информационной революции. Особенно в такой области, которая вызывает наибольшее опасение с точки зрения влияния на внутриполитическую стабильность в России. Я имею в виду социальные сети и их преступное использование.

Прежде всего нужно сказать о том, какое значение – политическое, социальное и правовое – приобрели социальные сети в последние два десятилетия. Они превратились в оружие, которое может быть использовано против институтов государства, как это произошло в 2020 г. в США и 23 января 2021 г. в России.

Напомню, к началу нового столетия социальные сети превратились фактически не только в средства массовой информации и дезинформации, т.е. в манипулируемые СМИ, но и в *средства силовой политики.*

Социальные сети имеют потенциал, с помощью которого можно коснуться каждого аспекта национальной безопасности, в том числе сбора и проверки информации в открытом доступе с открытым исходным кодом, замеров и влияния на общественное мнение, распространения «коммуникации рисков».

Особенный аспект, который вызывает сегодня озабоченность правоохранительных органов, – это соцсети как источник информации.

Отдельный аспект – исследования в социальных сетях. Мы получили колоссальные возможности, на порядок увеличили возможности коммуникации, экономим и тратим время как нам нравится. Но есть и обратная сторона. В социальных сетях стали изучать нас. А данные, которые получают во время таких исследований, пытаются использовать для влияния на менее продвинутые социумы. И уязвимым звеном становится молодежь.

Отдельный вопрос – *социальные сети как информационный канал экстремистского материала.* Как известно, существует два способа совершения экстремистских преступлений с использованием компьютерных сетей, которые включают в себя:

1) изготовление и распространение (манипулирование) посредством телекоммуникационных сетей, и в первую очередь сети «Интернет», информационной продукции, запрещенной российским законодательством и противоречащей интересам национальной безопасности государства, в целях оказания информационно-психологического воздействия на массовые аудитории граждан;

2) использование компьютерной техники и информационных технологий в целях организации и последующего руководства деятельностью экстремистских групп и сообществ, а также создания условий для совершения преступлений экстремистской направленности.

В сети «Интернет» чаще всего можно обнаружить следующие виды экстремистской информации:

программные документы различных групп, содержащие информацию, побуждающую к насильственному изменению конституционного строя и нарушению целостности России;

материалы пропагандистского характера, направленные на утверждение исключительности и превосходства русских, неполноценности граждан по признаку их отношения к религии, социальной, расовой, национальной, религиозной или языковой принадлежности и т.п.;

разнообразные сведения о способах изготовления самодельных взрывных устройств, совершения преступлений террористического характера.

Особенно беспокоит тот факт, что такую информацию с помощью интернет-ресурсов можно найти быстро и беспрепятственно.

Экстремизм в современной России в основном носит закрытый, завуалированный характер. В скрытую форму существования его вынуждают уходить все более строгие нормы закона в отношении экстремизма и прежде всего его политической формы. Однако за этим не следует, что экстремистские сообщества прекратили свою деятельность. Они всего лишь адаптируются к

изменяющимся условиям политико-правового пространства. Более того, по мере ужесточения законов, направленных на борьбу с экстремизмом, они используют более изощренные формы и методы работы, продолжая оказывать воздействие на пользователей социальных сетей.

Отдельная тема – *политические манипуляции* с использованием социальных сетей. Цветные революции, которыми принято называть массовые уличные беспорядки с яркой политической окраской, направленные на смену режима в определенной стране, являются одним из примеров манипуляции с социальными сетями. Наиболее деструктивно вовлечение в противоправные действия с призывами к участию в незаконных митингах несовершеннолетних и молодежи.

Следует констатировать, что относительно невысокая раскрываемость преступлений в информационной сфере требует принятия адекватных мер, направленных на повышение квалификации сотрудников правоохранительных органов, более глубокое освоение ими современных криминалистических методик.

Выполнить данную задачу возможно путем включения в образовательные программы высшего юридического образования разделов, посвященных тактике и методике расследования таких преступлений, а также путем корректировки тематических планов профессиональной переподготовки, повышения квалификации и специализации сотрудников правоохранительных органов.

К подобным мерам подталкивают и изменения в структуре информационной преступности.

Наши исследования показывают, что во многом успешность борьбы с преступлениями в информационной сфере определяется наличием необходимых наднациональных правовых документов, направленных на регулирование межгосударственных отношений по противодействию информационной преступности.

Востребованность международного сотрудничества в сфере противодействия использованию информационно-коммуникационных технологий в преступных целях вызвана трансграничной природой сети «Интернет», которая существенно затрудняет обеспечение цифрового суверенитета Российской Федерации.

Определенный прогресс в укреплении межгосударственных отношений связан с разработкой по инициативе Российской Фе-

дерации международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях.

Применение цифровых технологий в борьбе с преступностью может приобретать самые разнообразные формы, однако очевидно, что ее результативность напрямую зависит от повышения уровня технологической безопасности в информационной сфере.

Неслучайно Доктрина информационной безопасности Российской Федерации предполагает ликвидацию зависимости отечественной промышленности от зарубежных информационных технологий и средств обеспечения информационной безопасности, а также, что принципиально важно, развитие национальной системы управления российским сегментом сети «Интернет».

Несмотря на дистанционный формат сегодняшней конференции, уверена, ее насыщенная программа (а у нас свыше 170 заявок на выступления) и высокий профессионализм участников обеспечат творческую научную атмосферу, обмен знаниями и опытом специалистов из разных регионов России.

Хочу пожелать успешной и плодотворной работы участникам форума!

С.А. Бессчасный,
начальник Главного управления
правовой статистики и информационных
технологий Генеральной прокуратуры
Российской Федерации

Вступительное слово

Уважаемый Анатолий Вячеславович, уважаемые участники конференции! Позвольте поприветствовать вас и поблагодарить за возможность выступить перед широким кругом профессионального сообщества, тем или иным образом вовлеченного в вопросы противодействия киберпреступности.

Действительно, тема, которую планируется обсудить на конференции, заслуживает самого пристального внимания. Сейчас сложно представить какую-либо сферу общественных отношений, которой еще не коснулась цифровизация. Темпы расширения информационного пространства и внедрения технологий в повседневную жизнь граждан за последние 10–15 лет впечатляют. При этом современные интернет-технологии используются преступниками во всем мире и Россия в этом плане не исключение.

Данные уголовной статистики за последние 5–6 лет свидетельствуют о кратном росте массива киберпреступлений как в абсолютных, так и в относительных величинах. С 2015 г. общее число выявленных в стране преступлений сократилось на 13%, в то время как преступность в сфере информационных технологий возросла более чем в 11 раз (с почти 44 тыс. до 510 тыс.). Каждое четвертое зарегистрированное в прошедшем году преступление в той или иной мере было связано или совершено с использованием цифровых технологий. В структуре преступности их доля увеличилась с 2 до 25%. В Ханты-Мансийском автономном округе, к примеру, до 40%.

По абсолютному числу зарегистрированных преступлений лидерами по понятным причинам являются наиболее крупные субъекты – Москва (54,7 тыс.), Санкт-Петербург (19,5 тыс.) и Краснодарский край (19 тыс.).

Чаще всего противоправные посягательства с использованием цифровых технологий совершаются путем кражи или мошенничества.

В целом уровень раскрываемости киберпреступлений невысокий, около 20% за прошлый год, в отдельных регионах и того ниже (Ленинградская область – менее 11%, Севастополь и Смоленская область – менее 12%).

Наряду с проблемой установления лиц, совершивших киберпреступления, необходимо отметить невысокие показатели выявления преступлений в сфере компьютерной информации (гл. 28 УК РФ). В структуре киберпреступности на такие преступления приходится менее 1% (4,5 тыс.). За последние 5 лет все реже выявляются преступления, связанные с созданием, использованием и распространением вредоносных компьютерных программ (с 974 до 371). К 2020 г. сошли на нет и без того редкие случаи квалификации деяния за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ).

Вместе с тем определенные положительные тенденции в правоприменительной практике все-таки имеются. В частности, с 2018 г. более чем вдвое (до 4 тыс.) возросло количество зарегистрированных случаев неправомерного доступа к компьютерной информации (ст. 272 УК РФ). Относительно предыдущих двух лет в 2020 г. чаще стали выявлять преступления, связанные с неправомерным воздействием на критическую информационную инфраструктуру Российской Федерации (22). Уголовная ответственность за такие деяния установлена с июля 2017 г. (ст. 274^1 УК РФ).

В сегодняшних реалиях констатации факта широкого распространения киберпреступности явно недостаточно. Учитывая ее трансграничный характер, на повестке дня должны стоять вопросы не только выявления и раскрытия киберпреступлений, но и активного формирования предупредительного импульса. Для этого прокурорам потребуется скоординировать деятельность правоохранительных органов. Важной составляющей выработки адекватных превентивных мер является качественная организационно-аналитическая деятельность.

Генеральной прокуратурой Российской Федерации ежемесячно подготавливаются информационно-аналитические материалы о состоянии преступности в стране, которые направляются в Совет Безопасности Российской Федерации и в Администрацию Президента Российской Федерации. Отдельным блоком освещаются результаты борьбы с киберпреступностью.

В то же время возрастает потребность в получении более подробных сведений о киберпреступлениях, в том числе о новых способах их совершения, социальном положении потерпевших, суммах причиненного им ущерба. Для получения и анализа таких данных может быть применен инструментарий государственной автоматизированной системы правовой статистики. Мероприятия по ее созданию находятся на завершающей стадии. Система должна стать интеграционной платформой для единого информационного пространства в сфере уголовно-правовой статистики.

После внедрения ГАС ПС на территории страны можно будет получить в онлайн-режиме информацию по уголовному делу с момента регистрации сообщения о преступлении до вынесения судебного решения.

Система постоянно развивается, дополняется новыми функциями. Имеется механизм контроля сроков принятия процессуальных решений, программа позволяет в автоматизированном режиме подготовить информацию по любому делу и сделать выборку нарушений по документам, в частности выборку киберпреступлений, в том числе совершенных в отношении определенных категорий граждан (социально незащищенных слоев населения, предпринимателей, несовершеннолетних), с картографическим отображением места совершения деяния. Для прокуроров это станет хорошим инструментом мониторинга и анализа оперативной обстановки на территории и позволит принимать своевременные, скоординированные с правоохранительными органами меры по противодействию таким посягательствам.

В.В. Меркурьев,
заведующий отделом
НИИ Университета прокуратуры
Российской Федерации,
вице-президент Российской
криминологической ассоциации,
доктор юридических наук, профессор

Вступительное слово

Уважаемые коллеги! Меня переполняет чувство благодарности за возможность проведения Всероссийской научно-практической конференции в рамках Долговских чтений руководству Университета прокуратуры Российской Федерации и лично Вам, Оксана Сергеевна, за бережное отношение к памяти бессменного лидера Российской криминологической ассоциации – ветерана органов и организаций прокуратуры доктора юридических наук, профессора, заслуженного юриста РСФСР Азалии Ивановны Долговой.

К нашему большому горю в прошлом году не стало всемирно известного российского ученого-криминолога и руководителя научной школы. До последних дней своей жизни Азалия Ивановна активно участвовала в научной и общественной жизни Университета прокуратуры Российской Федерации. Достаточно вспомнить прекрасно организованную прошлогоднюю конференцию на тему «Криминологические проблемы поведения несовершеннолетних и молодежи, пути их решения», проведение которой в стенах Университета инициировала А.И. Долгова.

Нам предстоит продолжить дело нашего учителя, научного руководителя и старшего товарища, в том числе развивать криминологию, повышать ее теоретический уровень, методическую надежность исследований, достоверность и социальную действенность выводов и рекомендаций для правоохранительных и иных государственных органов, решающих практические задачи борьбы с преступностью.

Думаю, много говорить об актуальности темы конференции нет необходимости, ее подсказала сама жизнь, события в нашей стране и за рубежом.

Во-первых, по предложению Президента Российской Федерации в 2021 г. в России проводится Год науки и технологий. Об этом стало известно в декабре прошлого года на заседании попечительского совета МГУ имени М.В. Ломоносова после общения главы государства с представителями высшей школы.

Во-вторых, с учетом развития обслуживания в онлайн-режиме, а значит, и искусственного интеллекта, и элементов информационных технологий в прошлом году количество преступлений в высокотехнологичных сферах возросло более чем на 70%.

В-третьих, чтобы своевременно реагировать на подобные вызовы, все сферы жизни, сферы деятельности государства должны быть пронизаны современными информационными технологиями, в том числе искусственного интеллекта. Это значит, что и в сфере выявления, предупреждения и пресечения правонарушений мы должны действовать симметрично и применять такие же инструменты, которые применяют правонарушители. Государство будет на уровне тех требований, которые к нему сегодня предъявляются, только тогда, когда научится применять цифровые технологии и искусственный интеллект на упреждение.

Не секрет, что современные технологии предполагают резкое изменение навыков и требований к знаниям даже для работы на том же рабочем месте в течение примерно пяти–восьми лет.

Поэтому важно наладить широкий обмен результатами научных исследований на разного рода дискуссионных площадках, конференциях, круглых столах и семинарах, а также внести существенные коррективы в систему повышения квалификации, которая позволит сотрудникам правоохранительных органов, научным и педагогическим работникам постоянно соответствовать по своему интеллектуальному потенциалу требованиям, предъявляемым новыми технологиями.

Инновационные приложения создают принципиально новые возможности для проведения цифровых расследований, включая сохранение, извлечение и анализ данных, которые содержатся в сети, а также в гаджетах, изъятых у преступников. Обо всем этом толково написано в новой книге Ю.Н Жданова и

В.С. Овчинского[1], которую Владимир Семенович Овчинский – один из старейших членов Российской криминологической ассоциации и соратник Азалии Ивановны Долговой презентовал для рассылки участникам нашего форума.

Книга посвящена актуальным вопросам влияния технологий новой промышленной революции на преступность. В работе использован новейший опыт правоохранительных органов разных стран в борьбе с киберпреступностью и другими противоправными проявлениями.

Заглянуть в завтрашний день образования и пообщаться с коллегами со всей России предлагают разнообразные школы уже с первых дней 2021 г., предоставляя возможность участникам за несколько дней онлайн-интенсива ознакомиться с трендами цифрового образования. О возросшей популярности подобных образовательных программ говорит число зарегистрировавшихся участников, превышающее несколько десятков тысяч ежемесячно.

Я приветствую участников нашего научного собрания, общее число которых превысило 150 человек, членов Российской криминологической ассоциации, ученых, аспирантов, адъюнктов, студентов и курсантов, а также практических работников из 25 регионов Российской Федерации: от Алтайского края и Владимирской области до Ханты-Мансийского автономного округа – Югры и Челябинской области, а также республик Беларусь и Абхазия.

От имени Правления Российской криминологической ассоциации поздравляю криминологов России с учреждением Долговских чтений, желаю успешной и плодотворной работы участникам форума!

---

[1] *Жданов Ю.Н., Овчинский В.С.* Киберполиция XXI века: международный опыт. М.: Междунар. отношения, 2020.

ДОКЛАДЫ И ВЫСТУПЛЕНИЯ НА ПЛЕНАРНОМ ЗАСЕДАНИИ

В.В. Меркурьев,
заведующий отделом
НИИ Университета прокуратуры
Российской Федерации,
доктор юридических наук, профессор

Цифровые технологии в общей организации борьбы с преступностью

Общая организация борьбы с преступностью с использованием цифровых технологий наравне с другими элементами охватывается понятием борьбы с преступностью как системной деятельности, включающей согласно концепции А.И. Долговой следующие элементы:

а) общая организация борьбы с преступностью;

б) предупреждение преступности как профилактика, предотвращение, пресечение;

в) правоохранительная деятельность[1] (рис. 1).

Новейшие исследования наглядно демонстрируют, что любые резонансные события общественной и политической жизни используются преступниками. Наметившиеся в предыдущие годы тенденции компьютерной преступности стали более выраженными в 2019–2020 гг. с усилением цифровизации общества, продиктованной развитием ситуации распространения коронавирусной инфекции и применением ограничительных мер.

Современные вызовы киберпреступности неоднократно отмечались руководством Генеральной прокуратуры Российской Федерации. Прежде всего это касается тенденций преступности в сфере информационно-коммуникационных технологий, ее количественных и качественных изменений.

---

[1] *Долгова А.И.* Научное обеспечение борьбы с преступностью и повышение криминологической культуры общества // *Долгова А.И.* Избр. тр.; Акад. Ген. прокуратуры Рос. Федерации. М., 2017. С. 24–25.

Вместе с тем легальное определение понятия компьютерной преступности, как и перечень анализируемых преступлений отсутствует. Статистические формы, содержащие соответствующие сведения, ежегодно дополняются под воздействием результатов научных исследований и практики реагирования на современные вызовы и угрозы. Сегодня раздел 11 «Сведения о преступлениях, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, выявленных и предварительно расследованных субъектами регистрации» формы федерального статистического наблюдения № 4-ЕГС включает 39 составов.

Рис.1

За последние годы количественные показатели зарегистрированных киберпреступлений поступательно возрастали. Сверхинтенсивная динамика отмечена в последние три года, когда количество зарегистрированных преступлений увеличилось почти втрое. В 2020 г. зарегистрировано 510 396 анализируемых преступлений, что составило четверть от общего количества зарегистрированных преступлений (2 044 221) (рис. 2). За счет возрас-

тания степени общественной опасности киберпреступности в ее структуре существенно увеличилась доля тяжких и особо тяжких преступлений, которая в 2020 г. составила 52,5% (267 613).

Прогноз развития именно такого сценария был сделан учеными Университета прокуратуры Российской Федерации в 2016–2017 гг. в ряде работ[1].

Сведения о преступлениях, совершенных с использованием информационно-телекоммуникационных сетей и в сфере компьютерной информации[2]

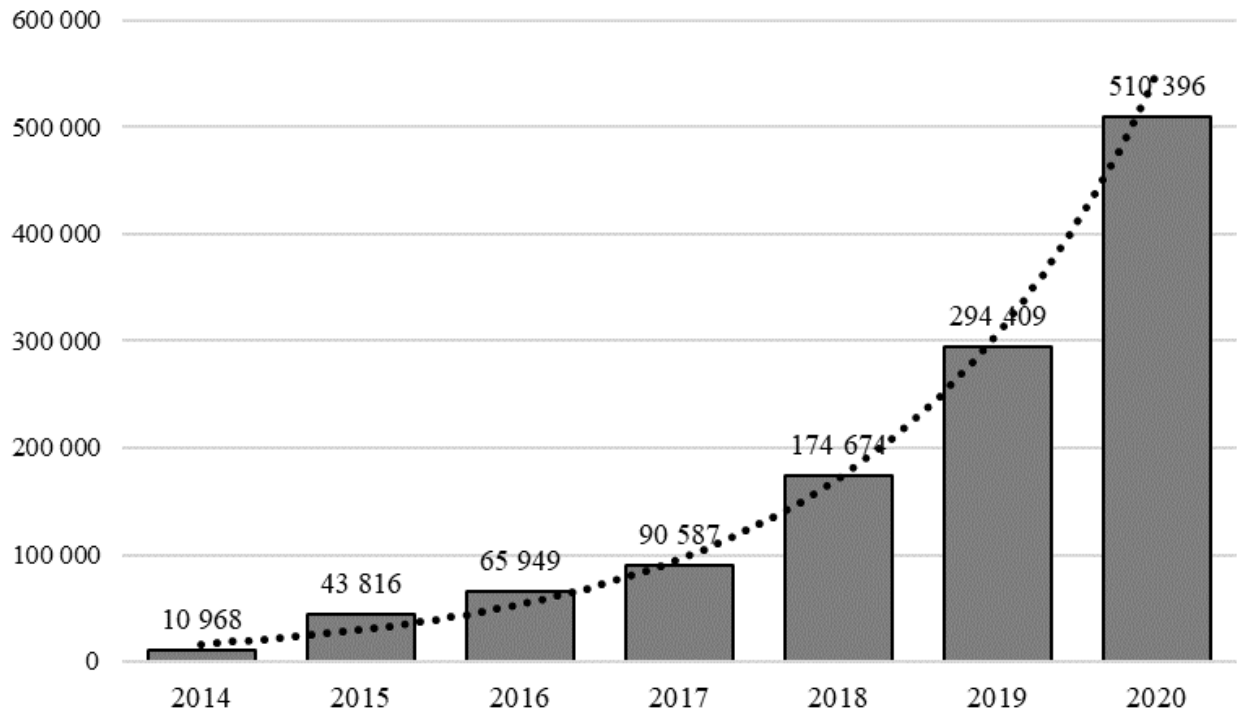


Рис.2

[1] См., например: *Ефремова М.А.* Уголовно-правовая охрана информационной безопасности: дис. … д-ра юрид. наук. М., 2017; *Меркурьев В.В., Ульянов М.В.* Проблемы реагирования на изменяющуюся преступность в контексте обеспечения национальной безопасности // Криминальные реалии, реагирование на них и закон / под ред. проф. А.И. Долговой. М.: Рос. криминолог. ассоц., 2018.

[2] Здесь и далее сведения о преступлениях, совершенных в сфере телекоммуникаций и компьютерной информации до 2017 г. включительно, приведены по форме статистической отчетности 1-ВТ, сведения о преступлениях после 2018 г. – по форме статистической отчетности № 4-ЕГС.

Подобная динамика обусловлена прежде всего ростом количества совершенных в сфере информационно-коммуникационных технологий мошенничеств (ст. 159 УК РФ) и краж (ст. 158 УК РФ) в 2020 г. более чем на 75%. Прирост незаконных производства и сбыта наркотических средств (ст. 228^1 УК РФ) составил 90,7%. Это основной сегмент зарегистрированной киберпреступности (см. таблицу).

Популяризация расчетов в безналичной форме привела к увеличению в 2020 г. количества преступлений, совершенных с использованием расчетных (пластиковых) карт (190 167 (+453,1%), компьютерной техники (28 653 (+56,9%) и средств мобильной связи (218 739 (+88,3%).

Наиболее часто информационно-коммуникационные технологии используются при совершении преступлений против собственности. Причем зачастую для совершения хищения злоумышленникам не требуется специальных познаний в области информационных технологий, что особенно относится к преступлениям с использованием платежных карт. Такого рода преступления в современных условиях стали типичными. С учетом этого очевидно, что одним из важных направлений противодействия их совершению является принятие комплекса мер по повышению уровня грамотности населения в сфере информационных технологий.

В то же время применение карантинных мер, вызванных глобальным распространением пандемии COVID-19, обусловило распространение технологий социальной инженерии, фишинга электронной почты, перехвата деловой переписки, кибератак на организации и отдельных лиц.

Сведения о зарегистрированных преступлениях, совершенных в сфере телекоммуникаций и компьютерной информации в период 2014–2020 гг. (форма № 4-ЕГС)

Статья УК РФ	2014	2015	2016	2017	2018	2019	2020
110 «Доведение до самоубийства»	сведения отсутствуют				13	4	10
110^1 «Склонение к совершению самоубийства или содействие совершению самоубийства»					18	11	9
135 «Развратные действия»							780
137 «Нарушение неприкосновенности частной жизни»					432	508	643
138 «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан»	43	42	30	42	143	180	306

138[1] «Незаконный оборот специальных технических средств, предназначенных для негласного получения информации»	352	369	320	434	289	125	172
146 «Нарушение авторских и смежных прав»	697	689	553	524	406	332	298
151 «Вовлечение несовершеннолетнего в совершение антиобщественных действий»	сведения отсутствуют				1	0	0
151[2] «Вовлечение несовершеннолетнего в совершение действий, представляющих опасность для жизни несовершеннолетнего»					1	0	1
158 «Кража»	2334	8449	9762	6945	32 668	98 798	173 416
159 «Мошенничество»	2187	13 483	32 875	51 513	90 664	119 903	210 493
159[3] «Мошенничество с использованием электронных средств платежа»	сведения отсутствуют		77	11	4242	16 119	25 820
159[6] «Мошенничество в сфере компьютерной информации»	995	5443	4329	2195	970	687	761
163 «Вымогательство»	сведения отсутствуют				1621	2090	3157
165 «Причинение имущественного ущерба путем обмана или злоупотребления доверием»	7	11	15	14	11	21	36
171[2] «Незаконные организация и проведение азартных игр»	37	475	720	825	875	842	747
172[2] «Организация деятельности по привлечению денежных средств и (или) иного имущества»	сведения отсутствуют				0	0	3
183 «Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну»	171	132	150	115	90	185	208
185[3] «Манипулирование рынком»	сведения отсутствуют				0	2	2
187 «Неправомерный оборот средств платежей»					203	433	804
205[2] «Публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма»					169	212	232
222, 222[1] «Незаконные приобретение, передача, сбыт, хранение, перевозка или ношение оружия…, взрывчатых веществ…»					68	56	76
ст. 228[1] «Незаконные производство, сбыт или пересылка наркотических средств…»					18 805	24 677	47 060
ст. 228[2] «Нарушение правил оборота наркотических средств или психотропных веществ»					0	0	0
ст. 228[4] «Незаконные производство, сбыт или пересылка прекурсоров наркотических средств…»					2	10	37
230 «Склонение к потреблению наркотических средств, психотропных веществ или их аналогов УК РФ»					5	1	7
234 «Незаконный оборот сильнодействующих или ядовитых веществ в целях сбыта»					106	129	392
242 «Незаконные изготовление и оборот порнографических материалов или предметов»	650	435	434	558	725	972	1372
242[1] «Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних»	758	529	408	508	548	704	545
242[2] «Использование несовершеннолетнего в целях изготовления порнографических материалов или предметов»	9	28	105	101	195	240	182
272 «Неправомерный доступ к компьютерной информации»	1151	1396	994	1079	1761	2420	4105
273 «Создание, использование и распространение вредоносных компьютерных программ»	585	974	751	802	733	455	371
274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации…»	3	12	3	2	5	4	0
274[1] «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации»	введена в 2018 г.				1	–	22
280 «Публичные призывы к осуществлению экстремистской деятельности»	сведения отсутствуют				253	257	340
280[1] «Публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации»					10	6	8
282 «Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства»					733	12	49

Преступники быстро воспользовались распространением инфекционных заболеваний и возросшим спросом на информацию и товары. С марта 2020 г. рядом компаний и финансовых организаций сообщалось о нарушениях. Компания «Лаборатория Касперского» подтвердила факты использования пандемии для придания вредоносным письмам убедительности.

Еще одним негативным последствием самоизоляции и увеличения интернет-активности стал рост количества фактов распространения в сети «Интернет» материалов, связанных с сексуальной эксплуатацией несовершеннолетних. Согласно данным Европола, ситуация вокруг пандемии предоставила преступникам доступ к широкой группе потенциальных жертв. Несовершеннолетние стали чаще пользоваться сетью при отсутствии контроля родителей как в свободное время, которого стало значительно больше, так и во время получения образования в рамках дистанционных учебных программ. Переместились в сеть и злоумышленники[1].

Актуальность данного мирового тренда для Российской Федерации в настоящий момент требует дополнительной проверки. В то же время имеющиеся данные позволяют говорить о большом сегменте подобных преступлений в истекший период. Количество выявленных преступлений, предусмотренных ст. 242[1] УК РФ, в 2014–2019 гг. варьировалось от 408 до 758, предусмотренных ст. 242[2] УК РФ, – возросло с 9 в 2014 г. до 240 в 2019 г., в 2020 г. – 195.

Расширение возможностей наркоторговли онлайн отражается на существенной доле и тенденциях роста преступлений в сфере незаконного оборота наркотических средств. Правоохранительными органами пресекается деятельность региональных и межрегиональных нелегальных интернет-магазинов. Как правило, механизм преступной деятельности предполагает наличие функционально обособленных структурных подразделений, большого числа участников с установленными обязанностями (закладчики, курьеры, операторы и др.), использование широкого набора программных продуктов в целях обеспечения конспирации, включая мессенджеры (Brosix, Vipole и др.) и сервисы обмена фотографиями (Imgur, Postimge и др.), не имеющие широкого распространения, VPN-сервисы, плагины, обеспечивающие шифрование переписки, электронные платежные системы[2].

---

[1] *Exploiting* isolation: offenders and victims of online child sexual abuse during the Covid-19 pandemic. European Union Agency for Law Enforcement Cooperation. 2020.

[2] *Земцова С.И.* Интернет-магазины, осуществляющие незаконный сбыт синтетических наркотических средств: дифференциация и характерные признаки // Вестн. Сибир. юрид. ин-та МВД России. 2019. № 1 (34).

С применением новых способов совершаются преступления в сфере компьютерной информации, а именно, предусмотренные ст. 272, 273, 274 и 274[1] УК РФ и включенные в гл. 28 УК РФ (Преступления в сфере компьютерной информации). В этом отношении нельзя не согласиться с мнением о том, что компьютерная преступность в последние годы вышла на качественно новый технологический уровень, что связано с научно-техническим прогрессом, эволюцией IT-технологий и формированием технотронного общества[1].

Совершение таких преступлений зачастую требует от злоумышленников наличия специальной технической подготовки. На фоне значительного увеличения количества почти всех преступлений в сфере информационно-коммуникационных технологий количественные характеристики преступлений, предусмотренных ст. 273 УК РФ, показывают отрицательную динамику (в 2020 г. выявлено 371 преступление). Проблемы их выявления традиционно увязывают с недостатками профессиональной подготовки сотрудников ведомств, призванных бороться с киберпреступностью.

Координация прокурором деятельности по борьбе с преступностью имеет существенное значение в реализации программ борьбы с преступностью и их корректировке. Не менее важное значение имеют совместно выработанные правоохранителями меры для стимулирования научных исследований в области оптимального использования цифровых технологий для борьбы с преступностью в высокотехнологичных сферах.

17 июля 2020 г. состоялось Координационное совещание руководителей правоохранительных органов Российской Федерации по вопросу «О состоянии работы правоохранительных и контролирующих органов по предупреждению, выявлению, пресечению и расследованию преступлений, связанных с посягательствами на безопасность в сфере использования информационно-коммуникационных технологий, включая критическую информационную инфраструктуру Российской Федерации».

---

[1] *Евдокимов К.Н.* Новые угрозы информационной безопасности России: от компьютерной преступности к анекселенктотичной технотронной преступности // Основные направления государственной политики России в сфере обеспечения национальной безопасности: материалы междунар. науч.-практ. конф. С. 57–65.

В контексте решения вопросов общей организации борьбы с преступностью важным представляется подп. 6.4 постановления, в котором предложено «организовать регулярное проведение межведомственных семинаров-совещаний с привлечением специалистов в сфере защиты информационной безопасности с целью обмена опытом по выявлению, пресечению, расследованию и предупреждению преступлений, совершаемых с использованием современных информационно-коммуникационных технологий».

Как известно, научная среда восприимчива к новым трендам и изменяющейся социальной, политической и экономической практике, в том числе в сфере использования технологий новой промышленной революции, как в преступных целях, так и в антикриминальной деятельности.

В 2020 г. в России прошла серия научных мероприятий[1] разного уровня, свидетельствующая о возросшем интересе к проблемам противодействия киберпреступности, с одной стороны, и появлении результатов научных исследований в области цифровых технологий – с другой.

Особо выделяется Четвертая Всемирная конференция по криминальным финансам и криптовалютам, прошедшая под эгидой Интерпола и Европола в ноябре 2020 г. По результатам конференции были приняты рекомендации, которые могут быть учтены в деятельности правоохранительных органов России и органов финансового надзора, которые в настоящее время готовятся к обеспечению финансовой безопасности в связи со вступлением в силу Федерального закона от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации». В частности, рекомендуются выпуск учебно-

[1] МНПК «Трансформация и цифровизация правового регулирования общественных отношений в современных реалиях и условиях пандемии» (Казанский филиал РГУП, 29.10.2020), МНПК «Актуальные проблемы международного сотрудничества в борьбе с преступностью» (Московский университет МВД России им. В.Я. Кикотя, 29.10.2020), МНПК «Геополитическая картина мира: угрозы и вызовы» (АТЦ СНГ, 09.11.2020), МНПК «Система ПОД/ФТ на страже глобальной и национальной безопасности: синтез права, экономики и IT» (Международный сетевой институт ПОД/ФТ Росфинмониторинга, 25.11.2020), ВНПК «Противодействие киберпреступлениям и преступлениям в сфере высоких технологий» (Санкт-Петербургская академия Следственного комитета Российской Федерации, 10.12.2020) и др.

методических материалов, проведение международных конференций, развитие государственно-частного партнерства в сфере противодействия отмыванию денег и финансированию терроризма, применение цифровых технологий в финансовых расследованиях[1].

Необходимо также отметить очередное заседание секции по проблемам нейтрализации внутренних угроз национальной безопасности научного совета при Совете Безопасности Российской Федерации на тему «О научных подходах к проблеме противодействия использованию информационно-телекоммуникационных технологий в преступных целях», которое состоялось в ноябре 2020 г. в Москве под руководством ректора Университета прокуратуры Российской Федерации профессора О.С. Капинус.

Решение секции имеет большое значение для организации, развития и координации научных исследований по проблемам использования цифровых технологий в борьбе с преступностью на предстоящий период. Одним из направлений, нуждающихся в научной проработке, отмечено создание международных инструментов противодействия использованию информационных технологий в преступных целях.

Отдельным вопросом стоит подготовка профессиональных кадров, переподготовка и повышение их квалификации, занимающая самостоятельную позицию в структуре общей организации борьбы с преступностью.

Хотелось бы обратить внимание на топ-10 перспективных специальностей в российских вузах: большая часть из них, в том числе гуманитарные, так или иначе связаны с цифрой. Об этом недавно рассказал Александр Куприянов, руководитель образовательной программы «Медиакоммуникации»[2].

Ну и последнее, мало подготовить и мотивировать молодых специалистов. Важно их в хорошем смысле удержать, получив максимальную пользу для Родины в деле борьбы с преступностью от их профессиональных знаний и компетенций. Не допустить «утечки мозгов».

---

[1] URL: https://www.europol.europa.eu/publications-documents/recommendations-4th-global-conference-criminal-finances-and-cryptocurrencies (дата обращения: 17.02.2021).

[2] URL: https://rg.ru/2021/01/02/top-10-perspektivnyh-specialnostej-v-rossijskih-vuzah.html (дата обращения: 13.01.2021).

Для этого государство должно пойти на определенные издержки, создавая для профессионалов в области цифровых технологий так называемую теплую капсулу. Она нужна для специалистов в области программирования и цифровых технологий. В качестве примера, к кому она может применяться, можно привести самого титулованного программиста мира, аспиранта Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики Геннадия Короткевича, уроженца Республики Беларусь, выигрывающего все известные соревнования по спортивному программированию, в том числе турниры Google, Facebook, IBM, «Яндекса», «ВКонтакте» и Mail.Ru Group.

Закончить хотелось бы словами из интервью Генерального прокурора Российской Федерации И.В. Краснова об участии прокуроров в качественно новой работе по противодействию коррупции в связи с регулированием выпуска, учета и обращения финансовых активов и цифровой валюты. Новая процедура проверки имущественного состояния должностных лиц запущена с началом действия закона о цифровых активах и криптовалюте, положения которого вступили в силу с 1 января 2021 г. и ввели в российское правовое поле названные объекты прав, создаваемые с использованием цифровых технологий. Справедливо будет сказать, что у нас есть не только киберполиция, но и киберпрокуроры[1].

[1] Интервью Генерального прокурора Российской Федерации Игоря Краснова «Российской газете». URL: http://www.genproc.gov.ru/smi/news/genproc/news-1894644/ (дата обращения: 17.02.2021).

И.Ю. Сундиев,
главный научный сотрудник
НИЦ № 2 ВНИИ МВД России,
доктор философских наук, профессор

«Токсичное» влияние цифросетевых структур на радикализацию молодежи

В условиях пандемической и ближайшей постпандемической реальности особую значимость для всех групп населения приобретают социальные сети и новые масс-медиа как основные источники жизненно важной информации. При этом уровень доверия к этим источникам у молодежи максимален[1]. Но надо помнить, что именно эти информационные каналы благодаря своим техническим возможностям наращивают скорость подачи и объемы информации. Как следствие, у потребителей этой информации снижается возможность сформировать свою версию происходящих событий: человек начинает жить в рамках навязанных ему интерпретаций. Тем самым информационная война в условиях пандемии не только не стихает, но и приобретает более изощренные формы. Необходимо отметить растущую медиазависимость терроризма и экстремизма: прогресс в медиа-технологиях меняет их природу, формы, методы вербовки, а также степень влияния на общественное мнение[2]. Важнейшими являются не столько технология съемки и передачи информации, сколько технологии формирования экстремистского и террористического контента[3], а также методов его распространения.

По исследованиям И. Ашманова и Н. Касперской[4], «на сегодняшний день в деструктивные течения в Рунете вовлечены порядка 5 миллионов аккаунтов российских подростков (35% от

---

[1] РСМД: Информационная безопасность в условиях пандемии COVID-19. URL: https://russiancouncil.ru/analytics-and-comments/analytics/informatsionnaya-bezopasnost-v-usloviyakh-pandemii-covid-19/?sphrase_id=35369216. (дата обращения: 09.04.2020).

[2] *Burke J.* How the changing media is changing terrorism // The Guardian. URL: https://www.Com/world/2016/feb/25/

[3] Контент (от англ. content – содержание) – это любое информационно значимое либо содержательное наполнение информационного ресурса или веб-сайта.

[4] *Ашманов И., Касперская Н.* Методическое пособие по выявлению признаков риска поведения в социальных медиа. М., 2019. URL: https://www.kribrum.ru/monitoring/.

общего числа подростков в России), и это число продолжает расти. За период с января 2018 г. по март 2019 г. обнаружен стабильно высокий, растущий деструктивный фон».

Исследование содержательной части контента масс-медиа и сети «Интернет» в постоянном режиме ведут ФСО, ФОМ и частные компании, входящие в крупные IT-концерны. Некоторые из них публикуют данные своих исследований с высокой периодичностью[1]. По отдельным проблемам исследования контента выходят диссертационные исследования, НИР вузов и научных центров[2].

Был принят ряд важных законодательных актов в сфере противодействия распространению негативного контента в СМИ и сети «Интернет», среди которых федеральные законы от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», от 28.07.2012 № 139-ФЗ и от 01.05.2019 № 93-ФЗ «О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» и отдельные законодательные акты Российской Федерации», от 28.12.2013 № 398-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации».

В аналитическом докладе «Фильтрация контента в Интернете. Анализ мировой практики»[3] названы следующие категории контента, которые должны подвергаться фильтрации:

политический контент (сайты оппозиционных и правозащитных движений, религиозных движений и сект, информация об этнических меньшинствах);

социально опасная информация (порнография, ЛГБТ-пропаганда, разжигание национальной и религиозной розни, призывы к насилию);

---

[1] Тенденции монетизации контента в Интернете. Медиапотребление в России-2019. Исследовательский центр компании «Делойт» в СНГ (Москва, сентябрь 2019 г.). URL: https://media.rbcdn.ru/media/reports/mediaconsumption-russia-2019.pdf.

[2] Профилактика экстремизма и террористического поведения молодежи в интернет-пространстве: традиционные и инновационные формы: метод. пособие. URL: https://minobrnauki.gov.ru/common/upload/library/antiterror/metodichka_soderzhanie_03.12.2018-1.pdf.

[3] Фильтрация контента в Интернете. Анализ мировой практики: аналит. докл. Фонд развития гражданского общества, 2013.

контент, связанный с национальной безопасностью (сайты террористических и экстремистских организаций, ресурсы военных противников, ресурсы с конфиденциальными данными и др.);

сайты и сервисы, нарушающие экономические интересы (файлообменные сайты и торент-трекеры);

специализированные интернет-инструменты и социальные сервисы (поисковые сервисы, социальные сети, онлайн-переводчики).

Лонгитюдные исследования, проводимые с конца 1980-х гг., зафиксировали стадийное «катастрофическое нарастание патофеноменов в детской популяции» – различных форм делинквентного и девиантного поведения (агрессивное поведение, токсикомания, речевые расстройства) – «в целом учебную и социальную неуспешность», а также ухудшение состояния здоровья школьников[1] (ныне молодых людей, включающихся в основные звенья производства и управления). Но патологический дизонтогенез в популяции проявляет себя и через описательные признаки.

Во-первых, это ограничение способности к целенаправленной деятельности (целеполаганию и самоорганизации), отсюда – невозможность нормального взаимодействия в социальной группе. Живое общение этих молодых людей со сверстниками вызывает неосознаваемые трудности, но, если его вести через технического посредника (гаджет-коммуникатор), проблема легко решается[2]. Так, невозможность принятия социальных ролей – как роли лидера, так и роли подчиненного в реале – компенсируется участием в компьютерной игре, где это легко реализуется в рамках стандартного сюжета. Еще один патологический признак – невозможность анализа и синтеза информационно-смысловых конструктов: Y-ки и Zеты не понимают переносных значений и игру слов, не воспринимают юмор и не смеются над анекдотами и шутками (опять же заменяя в виртуале мемами и демотивато-

---

[1] *Семенович А.В.* Нейропсихологическая коррекция в детском возрасте. Метод замещающего онтогенеза: учеб. пособие. М.: Генезис, 2007. С. 33.

[2] В течение дня поколение Z проводит онлайн более семи часов – 3:45 с компьютера и 4:01 с телефона (данные Global Web Index).

рами)[1]. В свою очередь, отсутствие результатов социально значимой деятельности приводит к потере обратной связи – индивид становится склонным значительно завышать самооценку (эффект Даннинга–Крюгера)[2] и не может реально соотносить свои результаты с реальными результатами деятельности других.

Во-вторых, это утрата эмпатии – эмоционального сострадания (восприятия чужой боли физической и душевной как своей собственной); эмпатия – важнейшее свойство для формирования морально-нравственных качеств личности, без которых общество не может развиваться. Сюда же можно отнести и повышение порога тактильной и болевой чувствительности (вплоть до клинических феноменов нечувствительности к душевной боли): толстокожесть, непробиваемость, черствость.

В-третьих, это утрата пассионарности – отсутствие «избыточной» психофизиологической энергии – «тонуса» (ответственна ретикулярная формация головного мозга), необходимого для нормальной социальной жизни – социальных свершений.

В-четвертых, это снижение либидо (либо инверсия и патологические влечения), вызванное незрелостью, а значит, функциональной недостаточностью стволовых отделов головного мозга (особенно ретикулярной формации). Если X и Y были «живчиками», то Z «не проявляют непреодолимого интереса» к противоположному полу (заменяя суррогатным или виртуальным сексом, тем более что непосредственное общение затруднено или невозможно в силу несложившихся коммуникативных качеств. Они не стремятся к семейной жизни, тем более «заводить детей», – это просто «неинтересно» и «противно». Отсюда – движение childfree – пожить для себя любимого.

В-пятых, это упрощенное представление о реальности. Поскольку отсутствует необходимая дифференциация «функциональных блоков мозга», картина мира строится из «крупных пик-

---

[1] Американские ученые Нейл Хоув и Уильям Штраус предложили в 1991 г. теорию поколений, согласно которой каждые 20–25 лет появляется новое поколение людей, которое отличается от предыдущих привычками, характером, ценностями и целями: молчаливое поколение (в 1923–1943 гг.); беби-бумеры (в 1943–1963 гг.); поколение X (в 1963–1984 гг.); поколение Y (в 1984–2004 гг.); поколение Z (в 2004 г. и младше).

[2] *Kruger J.; Dunning D.* Unskilled and Unaware of It: How Difficulties in Recognizing One's Own Incompetence Lead to Inflated Self-Assessments (англ.) // Journal of Personality and Social Psychology. 1999.

селов», а не предстает в «качественном» высоком разрешении. Поэтому такой ребенок, «внезапно» ставший взрослым, «не видит проблемы» и «сложностей» в любой области, не различает препятствий и возможных трудностей – целеполагание не работает, а огрубленный «образ цели» долго не удерживается вниманием[1].

В-шестых, это психологическая лабильность: из-за недоформированности «тормозных центров» лобных отделов – склонность к социальным девиациям, суицид, агрессия. Поскольку девиации скомпенсировать невозможно (перенести нагрузку на другие сопряженные отделы мозга), «онижедети» легко вовлекаются в деструктивные процессы – становятся орудием для социальной деструкции[2].

Еще один патологический феномен, характерный для Zетов, – возникновение «роевой» неспецифической (нечеловеческой) субъектности. Недостаточность «недостроенных» функциональных блоков мозга компенсируется через сетевые взаимодействия (через современные средства электронной коммуникации – интернет-мессенджеры). Можно сказать, что сеть как форма организации позволяет заместить недостающие функции полноценной социальной субъектности: «Сеть – …структура, в которой отсутствует единый центр (лидер, доминант), так что ее поведение является результатом кооперативных взаимодействий между элементами (узлами), среди которых могут быть несколько частичных лидеров с ограниченным воздействием на систему»[3]. Свойства сети антагонистичны свойствам социальных систем:

---

[1] Удержание образа будущего требует напряженной работы лобных отделов мозга – вытормаживать мешающие, борющиеся за доминирование другие информационные блоки. Отсюда и невосприимчивость к различным эстетическим формам, «эстетическая слепота» и «когнитивная слепота».

[2] По мнению американского исследователя М. Хогга, «такие люди легко становятся фанатиками и радикалами. …Людям всего лишь нужен кто-то, кто скажет им, что делать. … источником информации и влияния в большинстве случаев становятся интернет-веб-сайты, социальные сети, каналы в Twitter, подкасты и многое другое. Интернет – идеальное место для избавления от дискомфорта, связанного с неуверенностью в себе… В интернете можно с легкостью найти группы, которые малодоступны в обычном мире. …В этих замкнутых социальных вселенных определяются контуры «истины».

[3] *Олескин А.В.* Децентрализованные сетевые структуры в экономической и политической сферах. Сетевой социализм и сетевая меритократия // Сайт С.П. Курдюмова «Синергетика». URL: http://spkurdyumov.ru/networks/decentralizovannye-setevye-struktury-v-ekonomicheskoj-i-politicheskoj-sferax-setevoj-socializm-i-setevaya-meritokratiya/2/

если системообразующим фактором для «сборки» социальных субъектов является результат действия, то сеть не имеет всего этого и организуется только для того, чтобы иметь возможность и далее воспроизводить себя саму – максимально разрастаться («мерцает» ситуативно). Ключевая роль в управлении поведением и создании «молодежного роя» принадлежит соцсетям, особенно компании Facebook, которой принадлежат также приложения WhatsApp и Instagram. Как работает управление массами? СМИ и блогеры чутко реагируют на любое изменение алгоритмов Facebook и Google, стараясь под них подстроиться. Так алгоритм задает даже самым «независимым» из них повестку, поощряет показами «правильный» контент, убирает с глаз долой «неправильный», а порой и просто отправляет источник неугодной информации в «бан». Создатель алгоритма YouTube Кристос Гудроу в интервью одному из научных подкастов проговорился, рассказав, как система анализирует содержание видеоматериалов. Алгоритм добавляет просмотров тем из них, которые соответствуют общепринятым версиям, и «задвигает» тот контент, который не соответствует.

Ответственное социальное поведение при патологическом дизонтогенезе становится невозможным: утрата черт социальной субъектности приводит к тому, что индивиды легко вовлекаются в деструктивную социальную деятельность через широкий спектр новых форм специфической сетевой организации.

Новые формы девиантного поведения поколений Y, Z	**Дизонтогенетические патофеномены**
Скулшутинг	Психологическая лабильность, отсутствие эмпатии
Буллинг	Отсутствие эмпатии
Троллинг	Перенаправление эвристики и творческих способностей в виртуальную область, отсутствие эмпатии
Колумбайн	Отсутствие эмпатии, невозможность нормального взаимодействия в социальной группе

Суицидальные квесты	Психологическая лабильность
Убер-терроризм	Психологическая лабильность, отсутствие эмпатии, невозможность нормального взаимодействия в социальной группе, упрощенное представление о реальности
Протестные акции и флэшмобы	Психологическая лабильность, упрощенное представление о реальности
Чайлдфри, гомосексуализм и др.	Снижение либидо, инверсия либидо

Современный медиа-контент перестал быть исключительно текстовым, в нем все больше преобладает визуальность, что обеспечивает ему большую аудиторию. Преобладание визуальной информации над текстовой в традиционных СМИ, а также в различных типах рекламы интернет-пространства свидетельствует не только о возникновении нового способа общения, но и о глобальной трансформации стиля мышления массовой аудитории.

Цифровой мир формирует новый тип восприятия, отличный от традиционного текстового или книжного. Для обозначения нового типа сознания в середине 1990-х гг. в науке было введено понятие «клиповое сознание/мышление». Как сформулировал К.Г. Фрумкин, «суть клипового мышления заключается в том, что современный человек умеет и любит быстро переключаться между разрозненными смысловыми фрагментами. Обладателям клипового восприятия свойственна большая скорость обработки информации и способность к многозадачности. Эта многозадачность вызвала к жизни и такие феномены, свойственные современному человеку, как рассеянность, гиперактивность, дефицит внимания и предпочтение не текстовой, а образной информации»[1]. Клиповая культура и клиповое сознание, а некоторые называют его «клиповым мышлением», присущие «цифровым

[1] *Фрумкин К.* Откуда исходит угроза книге // Знамя. 2010. № 9. URL: https://magazines.gorky.media/znamia/2010/9/otkuda-ishodit-ugroza-knige.html.

аборигенам», Элвин Тоффлер[1] рассматривает как последствия формирования новой инфосферы, в которой до невероятных размеров возрос поток информации. Клиповое сознание выступает некоей защитной реакцией человека, который пытается освоить огромный объем передаваемых сообщений. Мозг такого человека, не успевая переработать всю информацию, обрушившуюся на него, отбирает только яркие «фрагменты» информационного «поля», повседневно скрывающего от человека реальную действительность. Для большинства современных молодых людей бумажная книга – это сложно, скучно и неудобно. Наиболее приемлемы форматы Twitter, Instagram, TikTok, в которых доминирует фиксированное число читаемых знаков, фото, коротких видео. Активная визуализация провоцирует неосознанные действия, которые потом, в «оправдание», будут «рационализированы» рассуждениями об их необходимости.

Сетевая коммуникация способствует удовлетворению таких базовых психологических потребностей, как:

спасение от одиночества и получение психологической поддержки;

сохранение существующих отношений;

поиск новых друзей, присоединение к виртуальному сообществу;

привлечение внимания, повышение статуса;

получение информации о людях, событиях, возможностях;

развлечение и регуляция эмоций.

Люди чаще всего ищут в сетевом общении ощущение психологического благополучия. Чем сильнее выражено чувство одиночества у человека, тем больше уровень его сетевого общения. Ощущение одиночества может возникать у индивида как при застенчивости, так и в ситуациях, когда он подвергается остракизму. Этим можно, например, объяснить высокую потребность в сетевом общении между трудовыми мигрантами, находящимися в чужой для них стране. Индивид обращается к возможностям сети для поддержания психологической близости в группе, для социальной поддержки. Именно эти специфические свойства сетевого общения активно используются террористиче-

[1] *Тоффлер Э.* Эра смещения власти. URL: http://www.df.ru/~metuniv/consor/POWER1.html.

скими и экстремистскими организациями. «Классической» можно считать схему вовлечения, состоящую из двух этапов.

На первом этапе общения в социальных сетях потенциальные объекты для вовлечения в экстремистские и террористические организации подвергаются убеждающей коммуникации и навязыванию им (отдельным реципиентам и группам) специфической системы ценностей через контент общения. Общий контекст такого воздействия выстраивается на продвижении стереотипов, предрассудков и предубеждений, разделяющих людей на «своих» и «чужих». Под воздействием такого рода коммуникации реципиенты постепенно меняют свои установки и поведение. На следующем этапе происходит селекция: реципиенты, проявившие высокую восприимчивость к предлагаемым идеям и ценностям и обладающие необходимыми способностями, вовлекаются в данные сообщества и становятся его членами. Их сознание подвергается насильственному убеждению, запускается механизм контроля сознания членов лидерами этих подгрупп. Технологии деструктивных сообществ в сочетании с современными возможностями коммуникации воздействуют на сознание молодых людей, трансформируют их мировоззрение и установки, изменяют их личность, превращая в орудие для реализации деструктивных целей и задач сообщества[1]. Реципиенты с выраженной психопатологией, психологически неустойчивые, с низким уровнем социально-нравственного развития становятся объектами бесструктурного и бесконтактного воздействия и ориентированы в основном на акции насыщающего террора[2].

Поскольку общество как системное построение в норме стремится к оптимуму («золотое правило саморегуляции»[3]), экстремальные психосоциальные события (в данный момент – пандемия), требующие мобилизации, вытесняют и вытормаживают «традиционные» возможности экстремистской и террористиче-

---

[1] Подробнее см.: *Лири Т., Стюарт М. и др.* Технологии изменения сознания в деструктивных группах / пер. с англ.; под ред. И. Митрофановой. СПб.: Экслибрис, 2002.

[2] Подробнее см.: *Сундиев И.Ю., Смирнов А.А., Андрюхин Н.Г.* Бесструктурные и бесконтактные способы вовлечения молодежи в террористическую и экстремистскую деятельность // Науч. портал МВД России. 2018. № 2.

[3] *Анохин П.К.* Узловые вопросы теории функциональной системы. М.: Наука, 1980. С. 96, 99, 119, 130–131.

ской деятельности, которые приобретают формы латентного существования.

Важно и то, что все медиапространство оказывается тотально занятым обсуждением социальных проблем экстремума и для одной из ведущих составляющих современной экстремистской и террористической деятельности – широкого медийного освещения – в нем практически не остается места. Единственными возможными формами представляются насыщающий террор и «новаторские» разработки с применением современных интернет-мессенджеров.

Эффективно противодействовать негативному контенту, способствующему вовлечению молодежи в деструктивную деятельность посредством масс-медиа и сети «Интернет», необходимо комплексно, в первую очередь с помощью организационно-правовых, информационных и оперативно-розыскных мер.

Меры организационно-правового противодействия ориентированы на криминализацию появляющихся видов преступного поведения, а также на реализацию принципа неотвратимости наказания за вовлечение молодежи в деструктивную деятельность, за совершенные подростками в результате такого вовлечения правонарушения и (или) преступления.

Так, в июле 2016 г. принят Федеральный закон № 374-ФЗ «О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» (далее – ФЗ № 374), который содержит ключевые новеллы, имеющие отношение к нашей теме. В частности, дополнен перечень оперативно-розыскных мероприятий ОРМ «Получение компьютерной информации» (ст. 6 Федерального закона «Об оперативно-розыскной деятельности»), на операторов связи возложен ряд дополнительных обязанностей, позволяющих противодействовать негативному контенту, способствующему вовлечению молодежи в деструктивную деятельность посредством масс-медиа и сети «Интернет».

Кроме того, 7 июня 2017 г. вступил в силу Федеральный закон № 120-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального ко-

декса Российской Федерации в части установления дополнительных механизмов противодействия деятельности, направленной на побуждение детей к суицидальному поведению».

Принятие данного нормативного правового акта – важнейший шаг в деле противодействия лицам, распространяющим негативный контент и склоняющим в информационно-телекоммуникационных сетях несовершеннолетних к совершению суицида. Так, ст. 110 УК РФ «Доведение до самоубийства» дополнена частью второй. Квалифицирующими признаками, отягчающими ответственность, теперь являются доведение до самоубийства: несовершеннолетнего или лица, заведомо для виновного находящегося в беспомощном состоянии либо в материальной или иной зависимости от виновного; женщины, заведомо для виновного находящейся в состоянии беременности; двух или более лиц; группой лиц по предварительному сговору или организованной группой; в публичном выступлении, публично демонстрирующемся произведении, средствах массовой информации и информационно-телекоммуникационных сетях (включая сеть «Интернет»).

Кроме того, в Уголовный кодекс Российской Федерации введены ст. 110^1 и 110^2, содержащие новые способы криминальной активности: склонение к совершению самоубийства (ч. 1 ст. 110^1); содействие совершению самоубийства (ч. 2 ст. 110^1); организация деятельности, направленной на побуждение к совершению самоубийства (ст. 110^2).

Очевидно, что принятие указанных и ряда других законов расширяет правовые возможности правоохранительных органов по отслеживанию негативного контента в информационном пространстве.

Меры информационного противодействия основаны на разъяснении сущности негативного контента, побуждающего молодых людей к деструктивному поведению, и его общественной опасности, направлены на формирование стойкого неприятия молодыми людьми идеологии насилия, терроризма и экстремизма, суицида, криминальных субкультур АУЕ, ЛГБТ-движений и т.д. Кроме того, призваны привлекать молодых граждан к участию в противодействии деструктивному поведению.

В рамках информационного противодействия необходимо применять методы информационного реагирования и контрпропаганды, направленные против деструктивного поведения, включая распространение официальных информационных сообщений, опровержений в СМИ и сети «Интернет», проведение брифингов или пресс-конференций для СМИ, подготовку и распространение информационной продукции (фильмов, передач, статей, плакатов и т.п.), участие в дискуссиях на форумах и в социальных сетях, проведение разъяснительных бесед с общественностью, семьями пострадавших.

Необходимой предпосылкой проведения данной работы является выстраивание конструктивного взаимодействия с институтами гражданского общества и СМИ в целях противодействия вовлечению молодежи в деструктивную деятельность посредством распространения негативного контента в масс-медиа и сети «Интернет» и формирования в общественном сознании понимания необходимости бескомпромиссной борьбы с указанными угрозами безопасности.

Обозначенные методы должны дополняться методами информационно-пропагандистского, обучающего и воспитательного воздействия, включать в себя меры, направленные на формирование информационного иммунитета у молодежи к распространению идеологии насилия, суицида, экстремизма, терроризма, кибербуллинга, скулшутинга, АУЕ, ЛГБТ-движений и т.д.

Формами информационно-пропагандистского, обучающего и воспитательного воздействия могут выступать специальные занятия и учебные курсы в образовательных организациях, ведение разъяснительной работы в ходе религиозных мероприятий, распространение специальной учебной и популярной литературы, создание специализированной информационной продукции СМИ и интернет-сайтов информационно-разъяснительного и просветительского характера, организация культурных, спортивных и иных массовых мероприятий и др.

Рассматриваемая группа методов включает в себя не только методы противодействия деструктивной деятельности, но и меры стимулирования позитивной социальной активности молодежи, пропаганду социально значимых ценностей. Например, создание патриотических общественно-политических организаций, под-

держка их деятельности, предоставление материального и информационного ресурса в сочетании с организацией различных препятствий для деятельности лиц, вовлекающих несовершеннолетних в деструктивную деятельность посредством ИТТ, включая сеть «Интернет».

Меры оперативно-розыскного противодействия направлены на предупреждение, выявление и документирование деятельности лиц, распространяющих негативный контент, вовлекающих молодых людей в деструктивную деятельность посредством масс-медиа и сети «Интернет».

Меры оперативно-розыскного противодействия направлены на выявление в интернет-среде фактов распространения негативного контента и осуществление документирования преступных действий в целях привлечения виновных к ответственности.

Основным способом получения информации о вовлечении молодежи в деструктивную деятельность посредством распространения негативного контента через масс-медиа и сеть «Интернет» является мониторинг сети.

Данную задачу на практике выполняют подразделения по противодействию экстремизму МВД России.

Так, на Главное управление по противодействию экстремизму Министерства внутренних дел Российской Федерации возложено проведение мониторинга печатных и электронных средств массовой информации, а также сети «Интернет» в целях выявления правонарушений экстремистского характера[1].

Главным управлением и территориальными подразделениями по противодействию экстремизму на постоянной основе осуществляется мониторинг сети «Интернет», направленный на изучение общественных настроений, социально-политической напряженности, криминогенной и социально-экономической обстановки и получение упреждающей информации о факторах, которые могли бы дестабилизировать общественно-политическую и криминогенную обстановку в стране.

Другим важным инструментом противодействия использованию негативного контента масс-медиа, включая сеть «Интер-

[1] Подпункт 10.29 разд. III Положения о Главном управлении по противодействию экстремизму Министерства внутренних дел Российской Федерации, утвержденного приказом МВД России от 21.06.2011 № 698дсп.

нет», для вовлечения молодежи в деструктивную деятельность является мониторинг сетевой активности злоумышленников и привлеченных ими лиц. Помимо классических методов оперативно-розыскной деятельности для решения этих задач могут использоваться автоматизированный сбор и анализ информации в информационно-телекоммуникационных сетях по технологиям больших данных. Для этого используются технические средства СОРМ. Правовые основы применения СОРМ заложены в ст. 64 Закона о связи, которая предусматривает обязанности операторов связи и ограничение прав пользователей услугами связи при проведении оперативно-розыскных мероприятий, мероприятий по обеспечению безопасности Российской Федерации и осуществлении следственных действий.

Э.Б. Хатов,
профессор кафедры
Университета прокуратуры
Российской Федерации,
кандидат юридических наук,
доцент

О роли цифровых технологий в анализе преступности

Реальную угрозу охраняемым законом правам и свободам граждан, а также интересам общества и государства представляет преступность. При этом, как писал авторитетнейший криминолог И.И. Карпец, много лет руководивший Всесоюзным научно-исследовательским институтом проблем укрепления законности и правопорядка при Прокуратуре СССР, 100 лет со дня рождения которого исполняется в 2021 г., преступность – явление вечное, присущее любой формации и вплетенное в живую ткань общественного организма[1]. Следовательно, борьба с преступностью также является перманентной задачей государства, которая предполагает объединение усилий правоохранительных органов. Доктор юридических наук, профессор, заслуженный юрист РСФСР

[1] См.: *Карпец И.И.* Преступность: иллюзии и реальность. М., 1992. С. 91–92.

А.И. Долгова, памяти которой посвящен настоящий форум, как исходный, необходимый элемент борьбы с преступностью справедливо рассматривала информационно-аналитическое обеспечение этой деятельности[1], включающей обязательный анализ состояния преступности. Отметим, что систематическое научное изучение преступности в нашей стране существенно активизировалось со второй половины XX в., особенно с образованием в 1963 г. указанного Всесоюзного научно-исследовательского института (ныне НИИ Университета прокуратуры Российской Федерации) и принятием постановления ЦК КПСС «О мерах по дальнейшему развитию юридической науки и улучшению юридического образования в стране» в 1964 г.[2]

Поэтому вопросы качественного, своевременного и достоверного анализа состояния преступности перманентно решают не только ученые-криминологи, но и в первую очередь практические работники. Указанная позиция нормативно подтверждается Положением о координации деятельности правоохранительных органов по борьбе с преступностью, согласно которому правоохранительные органы осуществляют совместный анализ состояния преступности, ее структуры и динамики, прогнозирование тенденций развития (п. 5)[3]. Осуществляя уникальную координирующую функцию в сфере борьбы с преступностью, прокуроры также занимают центральное место в ее анализе, ежегодно представляя руководству страны доклад о состоянии законности и правопорядка в стране и о проделанной работе по их укреплению, который в основном посвящен анализу преступности и ее причин. Прокуроры также обязаны информировать об указанном руководство субъектов Российской Федерации, органов местного самоуправления и население.

Вместе с тем деятельность прокуроров по анализу преступности, как и информационно-аналитическая деятельность прокуроров в целом, нуждается в совершенствовании. В связи с этим

---

[1] *Криминология*: учеб. для вузов / под общ. ред. д-ра юрид. наук, проф. А.И. Долговой. М.: Норма, 2005. С. 91.

[2] См.: *Кузнецова Н.Ф.* Преступление и преступность. М.: Изд-во Моск. ун-та, 1969. С. 172.

[3] Утверждено Указом Президента РФ от 18.04.1996 № 567 «О координации деятельности правоохранительных органов по борьбе с преступностью».

издание приказа Генерального прокурора Российской Федерации от 16.07.2020 № 380 «О совершенствовании информационно-аналитической деятельности органов прокуратуры Российской Федерации» выглядит своевременным. Необходимость совершенствования работы по анализу преступности подтверждается прокурорами, обучавшимися на факультете профессиональной переподготовки и повышения квалификации Университета прокуратуры Российской Федерации, представляющими различные звенья системы прокуратуры. На занятиях, посвященных информационно-аналитической деятельности, отдельные слушатели среди проблемных вопросов называют объективную оценку и объяснение причин роста/снижения показателей преступности, особенно в ходе комплексных или отраслевых проверок организации работы по различным направлениям.

На наш взгляд, такие разногласия, возможно, объясняются еще и тем, что в работе прокуроров нередко используются устаревшие технологии сбора и анализа информации, не позволяющие достоверно установить причины изменения динамики преступности.

В чем суть анализа? Основанная на логике, эта работа позволяет получить некоторую новую информацию из имеющейся, выявив содержащиеся в ней скрытые знания, уменьшив тем самым уровень неопределенности. При этом в правоохранительной деятельности «неопределенность – ключевое понятие теории и практики социального управления и в моделях принятия правоохранительным субъектом решений понимается как наличие нескольких возможностей исходов каждой альтернативы в деятельности по обеспечению безопасности общества от угроз преступности»[1].

Конечно, такой анализ – дело непростое. Тем более непросто прогнозировать состояние преступности. Следует учитывать огромные массивы информации, учесть которые, особенно используя компьютер только как калькулятор, может не каждый.

В Концепции цифровой трансформации органов и организаций прокуратуры Российской Федерации до 2025 года (далее –

---

[1] *Андреев Н.А., Коробов В.Б.* Стратегическое мышление в управлении правоохранительной сферой. М.: ЮНИТИ-ДАНА, 2013. С. 88.

Концепция цифровой трансформации), утвержденной приказом Генерального прокурора Российской Федерации от 14.09.2017 № 627, подчеркивается, что недостаточность использования современных средств и методов комплексной обработки разнородных данных не позволяет обеспечить требуемый уровень аналитической поддержки деятельности руководителей органов прокуратуры.

Из-за этого создаются предпосылки риска принятия дефектных управленческих решений соответствующими руководителями органов государственной власти, местного самоуправления, которым регулярно в силу закона и Конституции Российской Федерации направляются прокурорские информационно-аналитические документы (информации и доклады о состоянии законности и правопорядка), что может оказать негативный эффект в самых различных сферах деятельности, не говоря уже о состоянии законности и правопорядка.

Обладая уникальными полномочиями в правоохранительной сфере, органы прокуратуры, координируя деятельность правоохранительных органов по борьбе с преступностью, реализуя функции уголовного преследования, прокурорского надзора, постоянно получают различные сведения, отражающие состояние преступности и правонарушаемости, анализируют их, выполняя комплексный анализ состояния законности и правопорядка в стране, итогов прокурорской деятельности, а также осуществляют прогноз основных тенденций состояния законности, динамики и структуры преступности.

Порядок такого анализа регламентирован приказом Генерального прокурора Российской Федерации от 16.01.2012 № 7 «Об организации работы органов прокуратуры Российской Федерации по противодействию преступности». Прокурорам поручено не реже двух раз в год проводить анализ состояния преступности, ее причин и условий, ей способствующих, для чего использовать статистические и иные данные, сведения контролирующих органов, материалы прокурорских проверок, уголовных, гражданских и арбитражных дел, дел об административных правонарушениях, результаты проверок обращений граждан, научных исследований, сообщения средств массовой информации, а также другие сведения, характеризующие криминогенную обстановку.

В связи с этим своевременное и оперативное извлечение актуальной и достоверной информации в гигантском массиве разрозненных, нередко не подтвержденных или неполных данных и ее качественный анализ становятся одной из важнейших задач практически во всех сферах деятельности прокуроров. Ее решение, по нашему мнению, возможно только за счет применения цифровых технологий, которые позволяют существенно оптимизировать процесс определения детерминирующих преступность факторов, делают реальным достижение предикативного анализа преступности.

Интернет, информационные системы, социальные сети, электронные мессенджеры стали частью не только повседневной жизни россиян, но и повсеместной практики правоохранительной и контрольной деятельности государственных органов[1]. Вместе с тем до настоящего времени сохраняется определенный дефицит подключения прокуроров к недостаточно распространенным современным информационным системам, например СМЭВ. Не единичны факты нестабильной работы ЕЗСПД (единой защищенной сети передачи данных), отдельных модулей ГАС ПС (государственной автоматизированной системы правовой статистики) в прокуратурах районного звена, имеются проблемы, связанные с избыточно сложным алгоритмом ввода данных, длительным открытием ресурсов, неудачной загрузкой сведений из баз данных других ресурсов либо с выдачей ошибок, препятствующих оперативному внесению сведений в отчетно-аналитическую форму портала ССТУ.РФ (сетевой справочный телефонный узел – закрытый информационный ресурс, портал приема обращений граждан), а также осуществлению мониторинга электронных баз данных и официальных ресурсов правоохранительных, контролирующих и иных органов государственной власти, местного самоуправления. Так, чтобы избежать зависания, сбоев программного обеспечения, коллеги из отдаленных прокуратур субъектов Российской Федерации стараются осуществить загрузку необходимых данных в утренние или вечерние часы, чтобы использовать разницу во времени с московским регионом.

---

[1] *Хатов Э.Б.* Состояние единого информационного пространства органов прокуратуры, иных правоохранительных, а также контрольно-надзорных органов и судов // Вестн. Ун-та прокуратуры Рос. Федерации. 2019. № 3. С. 39.

Предусмотренное проектом цифровизации органов прокуратуры создание интерактивной карты преступности Российской Федерации с возможностью локализации очагов преступлений и правонарушений, определения параметров формирования очагов («тепловая карта преступности») вплоть до отдельной улицы и дома в любом населенном пункте также значительно повысит качество ее анализа. Размещенная в настоящее время на сайте crimestat.ru электронная карта преступности пока информирует о показателях преступности лишь на региональном уровне, дифференцируя регионы на несколько групп.

Представляется, что указанные проблемы носят временный характер и объясняются начальным этапом процесса цифровизации, полное завершение которой планируется в 2025 г. Накопленный в течение нескольких лет опыт внедрения ГАС ПС в прокуратурах пилотных регионов доказывает решаемость поставленных задач и подсказывает необходимость более широкого использования цифровых технологий, внедрения искусственного интеллекта.

Прокурорам также требуется подключение к базе данных системы уличных камер видеонаблюдения, в том числе web-камерам в режиме реального времени. Не менее значимым было бы и создание на модернизированном портале прокуратуры полноценных геокарт правонарушений, а также обращений граждан в органы прокуратуры и т.п.

Актуальными являются идеи о разработке ведомственных аналитических программ, которыми можно управлять голосовыми командами, так называемых электронных помощников прокурора (электронных ассистентов)[1].

Использование цифровых технологий для обработки больших данных методом корреляции позволит, по опыту прокуроров Казахстана, точно определять, какие макроэкономические факторы (уровень безработицы, рост/снижение доходов населения, объемы банковских вкладов, демографические и иные социально-экономические показатели) детерминируют всплески преступности.

---

[1] *Хатов Э.Б.* Перспективы информационно-аналитической деятельности прокуратуры в условиях цифровой трансформации // Реализация Концепции цифровой трансформации органов и организаций прокуратуры в современных условиях: сб. материалов круглого стола (Москва, 11 июня 2019 г.) / Ун-т прокуратуры Рос. Федерации. М., 2019. С. 41, 44.

Таким образом, внедрение высокотехнологичного прокурорского надзора, координации деятельности правоохранительных органов с использованием цифровых технологий, предусмотренное Национальной программой «Цифровая экономика Российской Федерации», по сути, предполагает цифровизацию анализа состояния преступности.

Цифровые технологии способны не только поднять на качественно новый уровень достоверность и эффективность анализа состояния преступности, но и освободить от рутинной работы прокуроров, служебная нагрузка которых близка к предельной, следовательно, повысить эффективность их деятельности в целом.

В.Н. Исаенко,
профессор кафедры уголовного процесса и криминалистики Московского государственного областного университета (МГОУ), профессор кафедры Университета прокуратуры Российской Федерации, доктор юридических наук, профессор

Прокурорский надзор за исполнением законов при расследовании преступлений в условиях развития компьютерных технологий[1]

Несмотря на существенное сокращение в 2007 г. полномочий по осуществлению надзора за исполнением законов в оперативно-розыскной деятельности, а также за процессуальной деятельностью органов предварительного следствия и органов дознания, прокурор в соответствии с ч. 2 ст. 21 УПК РФ остается равно ответственным за надлежащее качество проверок сообщений о преступлениях, а также за качество работы по установлению и изобличению совершивших их лиц, т.е. за надлежащее ис-

[1] Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 19-011-00896.

полнение требований закона о раскрытии и расследовании преступлений.

В приказе Генерального прокурора Российской Федерации от 16.01.2012 № 7 «Об организации работы органов прокуратуры Российской Федерации по противодействию преступности», а также в других организационно-распорядительных документах надзор за исполнением законов в данной сфере рассматривается как одно из приоритетных направлений деятельности. При этом все более интенсивно внимание прокуроров акцентируется на информационной составляющей деятельности. Это закономерно связано с очевидной необходимостью внедрения и использования в прокурорской деятельности цифровых (компьютерных) технологий, в том числе в сфере надзора в досудебном производстве.

В свою очередь, в Концепции цифровой трансформации органов и организаций прокуратуры Российской Федерации до 2025 года констатируется необходимость повышения эффективности надзора путем внедрения современных и перспективных информационных технологий обработки информации во всех видах надзорной деятельности. Поэтому в обновленной редакции Квалификационной характеристики должности (квалификационных требований к должности) прокурора города, района и приравненного к ним прокурора занимающие их прокурорские работники обязаны совершенствовать навыки владения компьютерной и другой оргтехникой с учетом развития цифровой трансформации и информационных технологий, уметь пользоваться необходимым программным обеспечением, справочными информационными системами, электронно-образовательной средой[1]. Учитывая, что в прокуратурах этого уровня выполняется основной объем работы по надзору в досудебном производстве, данное требование приобретает особую актуальность.

В связи с очевидной необходимостью оптимизации прокурорского надзора в досудебном производстве за счет внедрения

[1] Квалифицированная характеристика должности (квалификационные требования к должности) прокурора города, района и приравненного к ним специализированного прокурора, утвержденная приказом Генерального прокурора РФ от 12.08.2010 № 316 «Об организации профессиональной переподготовки прокурорских работников, включенных в резерв кадров для выдвижения на должности прокуроров городов, районов и приравненных к ним прокуроров».

компьютерных технологий возникает вопрос о том, на каких участках этого направления надзора возможно их использование. Представляется, что перечень действующих систем прикладного программного и информационно-аналитического обеспечения прокурорской деятельности может быть расширен за счет разработки, апробирования и внедрения в практику ряда других.

В частности, представляется возможным осуществлять надзор за исполнением законов при приеме, регистрации и разрешении сообщений о преступлениях с использованием специально разработанных программ, базирующихся в том числе на основе творческой интерпретации идей Г.А. Густова[1], который предложил разрабатывать краткие и развернутые программы расследования в виде логически упорядоченных систем не только типовых задач расследования, но и их типовых решений. В настоящее время разрабатываемые и внедряемые в практику типовые частные методики расследования преступлений отдельных видов включают блоки действий по проверке сообщений об этих преступлениях. Типичность выполняемых при этом процессуальных и иных действий представляет, по нашему мнению, возможность разработать соответствующую программу, использование которой нацелено на проверку полноты их проведения в типичных исходных ситуациях. В реальности такая компьютерная программа (искусственный интеллект) может функционировать, если:

1) она используется для анализа и оценки материала проверки сообщения о преступлении с формальным составом;

2) объем и содержание совокупности установленных обстоятельств, их характеристики (параметры) позволяют отыскивать аналогичные сочетания в памяти компьютера;

3) в программу заложены соответствующие типичным встречающимся на практике ситуациям варианты обусловленных ими решений рекомендательного характера;

4) материалы проверки сообщения о преступлении представлены в оцифрованном виде (заявление о преступлении с описанием обстоятельств совершения преступления, объяснение заявителя с их детализацией и др.).

Прокурорской, судебной практикой выработан комплекс критериев, используемых при анализе и оценке доказательств, а

---

[1] *Густов Г.А.* Разработка и использование типовых криминалистических программ в работе по уголовному делу: метод. рекомендации. Л., 1989. С. 8–10.

также реагирования на нарушения законов при их собирании. Представляется, что при наличии в органах прокуратуры в настоящее время необходимых кадровых и технических возможностей эти материалы могут быть использованы для разработки и апробирования автоматизированной справочной системы (АСС) «Доказательства» как элемента информационного обеспечения прокурорского надзора в досудебном производстве. АСС может представлять, с одной стороны, разновидность информационной технологии, используемой на данном направлении прокурорской деятельности, а с другой – элемент его цифровой платформы.

Концептуально ее элементы (блоки) представляются в виде взаимосвязанных совокупностей: а) нормативных правовых актов (в первую очередь положений уголовно-процессуального закона, устанавливающих общие и частные условия производства отдельных следственных действий); б) материалов судебной практики, включая постановления и определения Конституционного Суда Российской Федерации, постановления Пленума, Президиума, определения Судебной коллегии по уголовным делам Верховного Суда Российской Федерации, отражающих правовую позицию о допустимости или недопустимости доказательств отдельных видов, а также оснований признания их судом недопустимыми; в) материалов прокурорской надзорной практики в досудебном производстве; г) типовых образцов требований прокурора об устранении нарушений закона при производстве следственных действий (если возможно их повторное проведение), а также постановлений о признании недопустимыми отдельных видов доказательств.

Предлагаемая АСС может быть средством освобождения прокурора от выполнения некоторых рутинных операций, одновременно позволяющим избежать направления в суд уголовного дела, по которому вывод органа предварительного расследования обоснован недопустимыми доказательствами.

Помимо предлагаемой АСС «Доказательства» представляется возможной разработка ее своего рода подсистемы «Заключение эксперта», имеющей несколько отличающуюся структуру. Необходимость ее разработки обусловлена тем, что заключение эксперта нередко является в суде доказательством, относительно которого возникает острая дискуссия государственного обвинителя и защитника. В силу того, что на государственного обвини-

теля возложено бремя опровержения доказательств стороны защиты о недопустимости доказательств, он должен быть всесторонне подготовленным к участию в полемике по этим вопросам. В свою очередь, ему (как и прокурору, осуществляющему надзор в досудебном производстве) может оказать действенную справочную помощь предлагаемая система. Представляется, что ее элементами (модулями, блоками) могут быть: 1) «Общие сведения» – информация о видах современных судебных экспертиз, перечнях разрешаемых ими в данный период вопросов и учреждениях, в которых они выполняются; 2) «Правовые позиции высших судов» – для выяснения вопросов: а) о правомерности назначения экспертизы, заключение которой подвергнуто оценке; б) о разрешении отдельных спорных вопросов, возникающих при оценке заключения эксперта, в том числе о его допустимости, о соблюдении права на защиту и др.; 3) «Методики судебно-экспертных исследований» – формируются во взаимодействии органов прокуратуры с судебно-экспертными учреждениями; 4) «Рекомендации по анализу выводов эксперта»; 5) «Экспертная терминология» – систематизированный перечень (тезаурус) разъяснений специальных терминов, наиболее часто встречающихся в заключениях экспертов отдельных специальностей (их расшифровка безусловно необходима, в частности, при поддержании государственного обвинения в суде с участием присяжных заседателей); 6) «Типовые образцы актов прокурорского реагирования на нарушения закона при назначении и производстве судебных экспертиз».

В современных условиях прокурору важно знать, в частности, правомерность назначения и проведения экспертиз отдельных видов, заключения которых нередко фигурируют в уголовных делах. В частности, таковыми являются заключения полиграфологических, нейро-психофизиологнических экспертиз по результатам исследования полиграмм тестирования свидетелей и подозреваемых, видео- и аудиозаписей допросов подозреваемых и обвиняемых с целью установления признаков лжи или достоверности в их объяснениях и показаниях, наличия или отсутствия признаков неправомерного воздействия на них. Обращает на себя внимание и то, что некоторые прокуроры не исключают такие заключения при утверждении обвинительного заключения, а госу-

дарственные обвинители представляют их суду в числе других обвинительных доказательств. При этом не учитываются материалы судебной практики, в которой устоялось отношение к таким заключениям.

Например, Краснодарский краевой суд, рассмотрев уголовное дело по обвинению В., осужденного Староминским районным судом Краснодарского края, в связи с апелляционной жалобой осужденного и его защитника, исключил из описательно-мотивировочной части приговора указание суда первой инстанции на заключение психофизиологической экспертизы потерпевшего. Свое решение краевой суд мотивировал тем, что выводы подобного исследования не могут быть признаны научно обоснованными, а оценка показаний участников процесса относится к компетенции суда[1].

Оставляя, что называется, за кадром научные аспекты возможности проведения подобной экспертизы, зададимся вопросами, которые отнюдь не являются риторическими: 1) может ли в принципе быть состоятельным ее заключение при отсутствии иных доказательств совершения подозреваемым, обвиняемым инкриминируемого ему преступления, объективно подтверждающих его преступную осведомленность об обстоятельствах его совершения; 2) какое обстоятельство предмета доказывания устанавливает подобная экспертиза, относящаяся именно к средствам доказывания, обстоятельства предмета которого четко названы в ст. 73 УПК РФ. Сталкиваясь с подобным заключением, участвующий в уголовном производстве прокурор сможет, обращаясь к предлагаемой справочной системе, объективно оценить возможность и перспективу его оставления в уголовном деле.

Одним из требований, предъявляемых к профессиональной подготовке прокурора города, района и приравненного к ним прокурора, является владение методикой расследования преступления, что также предусмотрено названной Квалификационной характеристикой. Полагаем, что компьютерные варианты частных методик расследования преступлений отдельных видов могут быть трансформированы в частные методики прокурорского

[1] Апелляционное определение Краснодарского краевого суда от 30.03.2020 по делу № 22- 3719/2020.

надзора за расследованием преступлений соответствующих видов. Безусловно, это потребует проведения определенного объема исследований с целью выделения таковых с параллельной разработкой названных комплексов, в том числе с использованием материалов обобщения судебной практики и прокурорского надзора.

Полагаем, что разработка, апробирование и внедрение предлагаемых методик в соответствующую прокурорскую практику целесообразны в качестве инструмента: а) всесторонней и объективной оценки полноты действий следователя, дознавателя на первоначальном и последующих этапах досудебного производства, а также оценки законности и обоснованности принятых на этих этапах процессуальных решений; б) принятия соответствующих характеру нарушений требований ч. 2 ст. 21 УПК РФ, допущенных следователем, дознавателем, правовых и организационных мер прокурорского реагирования на эти нарушения.

Ее использование предполагает вместе с тем совершенное знание прокурором не только норм уголовного и уголовно-процессуального законов, но и возможностей прикладной криминалистики, уголовной (криминалистической) регистрации, судебной экспертизы.

Предлагаемые компьютерные средства оптимизации прокурорского надзора могут быть многофункциональными, т.е. использоваться как прокурором, осуществляющим надзор в досудебном производстве, так и участвующим в рассмотрении уголовных дел судом, в работе по повышению квалификации и профессиональной переподготовке прокурорских работников, т.е. выполнять как контрольную функцию, так и функцию обучения, в том числе студентов образовательных организаций прокуратуры.

В юридической литературе обоснованно отмечается, что возможности компьютерных программ в расследовании не следует преувеличивать. Их создание и разработка не должны приводить к «автоматизации» следственного труда[1]. Точно так же не стоит преувеличивать возможности использования программного материала в осуществлении прокурорского надзора в досудебном

[1] См., например: *Косарев С.Ю.* История и теория криминалистических методик расследования преступлений: монография. М.: Юрлитинформ, 2020. С. 323.

производстве, представляющем собой в первую очередь мыслительную деятельность, постоянно сопряженную с оценкой и поиском оптимального и законного решения в конкретной ситуации правоприменения.

При определении возможностей использования компьютерных технологий прокурорскими работниками необходимо учитывать ряд факторов, причем не только современные правовые и технические возможности цифровизации надзорной деятельности, но и их менталитет, уровень правовой культуры и профессиональной готовности к использованию рассматриваемых технологий.

Тем не менее определенная модернизация прокурорского надзора в досудебном производстве с адаптацией ныне используемых правовых средств его осуществления к цифровой реальности – одна из частных задач, решение которой поможет, в свою очередь, решению общей задачи расширения цифровой составляющей прокурорской деятельности.

В.С. Овчинский,
советник Министра внутренних дел
Российской Федерации,
доктор юридических наук

Об угрозах квантовых компьютерных вычислений

Как сообщил в конце 2020 г. The Economist, квантовые компьютерные вычисления уже в скором времени могут иметь «революционное» воздействие на банки, а также на финансы, да и на всю нашу жизнь в широком смысле.

Квантовые компьютеры позволят увеличить прибыль за счет ускорения оценки активов, поиска более выгодных портфелей, сделают более точным алгоритмы обучения самих машин. Проведенное в июле 2020 г. испанским банком BBVA исследование свидетельствует, что квантовые компьютеры могут ускорить процесс оценки кредитоспособности, определить возможности для скупки акций с целью последующей перепродажи, ускорят

так называемое имитационное моделирование с помощью метода Монте-Карло, который широко используется в финансовой области для моделирования возможного поведения рынков.

Финансы – не единственная отрасль, рассчитывающая получить выгоду даже от небольших и нестабильных квантовых компьютеров, которые доступны в настоящее время. Очень многие сектора промышленности – от аэрокосмической до фармацевтической (не говоря уже о военной области) – также рассчитывают воспользоваться «квантовым преимуществом». Однако есть все основания полагать, что именно финансы смогут первыми найти такой способ.

Такие банки, как BBVA, «Ситигруп», «Джей-Пи Морган» и «Стандард чартед», создали исследовательские команды из специалистов по квантовым вычислениям и подписали соглашения с компьютерными фирмами. Эксперты консалтинговой фирмы «Бостон консалтинг груп» считают, что банки и страховщики в Америке и в Европе, по данным на июнь текущего года, наняли на работу более 115 экспертов – это большое количество даже в академической сфере для такой узкой специализации.

В некоторых банках сейчас больше докторов физических и математических наук, чем в университетах.

Когда же может произойти финансовая революция? По мнению одних экспертов, простые алгоритмы могут начать использоваться в течение 2021–2022 гг., по мнению большинства специалистов – в 2023–2025 гг.

Особенности квантовых компьютеров

Все, что делают современные компьютеры, включая искусственный интеллект, – это кодировка поступающей информации, превращаемой в нули и единицы, и их вычисление. Привычные нам вычислительные устройства – плод достижений физики последней четверти XIX в. и начала нынешнего. Они базируются на принципах классической физики.

Квантовый компьютер работает иначе, нежели привычный нам компьютер. В его основе лежат достижения самой быстроразвивающейся отрасли естествознания в XX – начале XXI в., а именно квантовой физики. В последние примерно 30–40 лет удалось не только открыть, но и научиться устойчиво воспроизво-

дить условия совершенно невероятного и до сих пор непонятного процесса, который называется *суперпозиция.*

В мире привычной нам физики и соответственно в компьютерах и смартфонах процессоры могут работать с двумя альтернативными возможностями, которые шифруются как 0 и 1. Минимальная единица информации в обычном компьютере – бит, т.е. способность принимать одно из значений – 0 или 1. Квантовый компьютер в отличие от традиционного способен работать в состоянии суперпозиции. Применительно к вычислениям это означает, что его элементарные вычислительные ячейки могут оперировать не только 0 и 1, но и во всех возможных промежуточных состояниях между ними. Казалось бы, какая разница, в одном состоянии или в двух и более пребывает вычислительная система. А разница огромная. Если квантовый компьютер имеет, например, 10 регистров, то он может пребывать одновременно в тысяче состояний. А в 20 регистрах – более 1 млн состояний и т.д.

Квантовый компьютер, или вычислительная физическая система, использующая законы квантовой механики, имеет примерно такое же сходство с традиционным компьютером, как лошадь с самолетом. И тот, и другой способны доставить путника из пункта А в пункт Б, и в этом они схожи. Однако в темпах и иных возможностях доставки самолет на порядки превосходит лошадь.

Собственно, знаменитый термин «квантовое превосходство» фиксирует простую и очевидную вещь. Квантовый компьютер на порядки превосходит по вычислительной возможности обычные двоичные вычислительные системы, включая суперкомпьютеры. Причем разница в возможностях исчисляется не разами, а тысячами и миллионами раз.

Пока в мире имеется единственный полноценный квантовый компьютер – 53-кубитный квантовый компьютер Google Sycamore, который смог решить задачу, недоступную для самых мощных «обычных» суперкомпьютеров. Если быть точным, у современного суперкомпьютера IBM Summit решение этой задачи заняло бы 20 000 лет, тогда как Sycamore выполнил все необходимые вычисления всего за 200 секунд. Принципиальное отличие системы Google от иных заявленных достижений в том, что математики, физики и прочие могут подать заявку и после рассмот-

рения будут допущены к работе на компьютере. На нем уже отработало большое число людей с высокой репутацией в мире программирования и математики. Тем самым он прошел общественную верификацию.

Еще одна принципиальная сложность в использовании квантового компьютера состоит в том, что он в некотором смысле воспроизводит механику расчетов, которая существовала в те, казалось бы, далекие времена, когда вместо чипов использовались лампы, а математика, лежащая в основе вычислений, носила непрерывный, а не дискретный характер. Практически это означает, что все программы, написанные для современных компьютеров, включая суперкомпьютеры, не подходят для квантового компьютера. В этой области пока только делаются первые шаги программирования. Все ныне работающие квантовые компьютеры, а они созданы в США, Китае, Южной Корее, Японии и в ЕС, – это специализированные машины, рассчитанные на определенный тип вычислений.

Иными словами, квантовый компьютер сегодня не может подобно смартфону сначала показать нам фильм, потом напомнить, что надо сходить в магазин, а в итоге провести расчеты оптимального выбора вложений в акции на рынках капитала. Пока все квантовые компьютеры – это специализированные, а не универсальные машины.

Полноценный квантовый компьютер – дело будущего. Пока, и об этом надо говорить четко и ясно, существуют лишь экспериментальные действующие макеты полноценных квантовых компьютеров. Макеты в том смысле, что они работать уже могут, но ориентированы на строго определенные операции.

Анализ динамики развития квантовых вычислений позволяет с уверенностью утверждать, что мы имеем дело с так называемой экспоненциальной технологией. В 2019–2020 гг. произошел перелом. Если еще пару-тройку лет назад наиболее продвинутые, имеющие за плечами выдающиеся достижения специалисты в области IT полагали, что практическое применение квантовых компьютеров – дело конца 2020-х – начала 2030-х гг., то сегодня они с уверенностью утверждают о приходе эры квантовых компьютеров буквально в течение ближайших четырех-пяти лет.

Решающее значение имеет то обстоятельство, что никто не хочет опоздать на этот праздник. Всех беспокоит, что оказавшийся первым в этой гонке сможет выбрать такой вариант: незаметно начать получать всю выгоду и не объявлять об этом всему миру.

Выгоды и угрозы квантовых компьютеров

Как любая технология новой промышленной революции, квантовый компьютер несет для общества серьезные выгоды и катастрофические угрозы. Он может преобразить банковское дело, создать мощную систему киберзащиты, может на порядок усовершенствовать систему защиты от любого военного нападения, а может стать страшным оружием в руках террористов или мафиозных структур.

Наиболее серьезные угрозы глобальной и национальной безопасности, экономике и повседневной жизни несет в себе использование квантовых компьютеров для взлома кодов. Специалисты по криптографии Агентства национальной безопасности США еще в 2015 г. опубликовали на сайте АНБ отчет, где выразили серьезную обеспокоенность перспективой появления работающих квантовых компьютеров, поскольку это может привести к чрезвычайно быстрой расшифровке многих использующихся сегодня криптографических алгоритмов. Представители АНБ отмечали, что вопрос разработки криптостойких алгоритмов, способных эффективно шифровать данные в эру квантовых компьютеров, актуален как никогда. По мнению специалистов агентства, вполне реально появление работающего квантового компьютера, существование которого поставит под угрозу сохранность государственных и коммерческих данных во всех сферах. Хотя время от времени в ведущих мировых медиа появляются статьи об угрозах квантовых компьютеров для международных расчетных систем, процессинговых компаний типа MasterCard, Visa и т.п., а также криптовалют и в первую очередь биткойна, реальная ситуация благоприятнее, чем описываемые сценарии.

Дело в том, что к настоящему времени разработаны и в 2023–2024 гг. будут готовы к практическому использованию так называемые постквантовые методы криптографии. Они базируются на сложнейшей математике, а их применение не позволяет

квантовым компьютерам вскрывать корпоративные и федеральные сети как консервный нож банку. Более того, во второй половине 2020 г. проведены испытания прототипов квантовоустойчивой системы шифрования, выстоявшей перед атакой квантового компьютера Goggle.

Главный недостаток систем постквантового шифрования – чрезвычайно высокая цена их разработки, огромные издержки, связанные с практической эксплуатацией для защиты данных, как хранящихся в базах данных, так и передаваемых от телекоммуникационных систем.

Самая большая угроза квантовых компьютеров мировой экономике и повседневной жизни состоит в следующем. Даже на начальной стадии квантовые компьютеры могут практически мгновенно сломать любой антивирусник и получить доступ, согласно мнению АНБ, примерно к 97% индивидуальных компьютеров, смартфонов и ноутбуков и не менее 65% – корпоративных. Поскольку постквантовое шифрование не только на стадии разработки, но и на стадии эксплуатации требует больших денег, оно без сомнения будет развернуто в 2022–2023 гг. для федеральных органов власти, систем национальной безопасности и правопорядка, в ведущих научных центрах и крупнейших компаниях. Причем далеко не во всех странах. Среди них будут безусловно США, Китай, Япония, Южная Корея и Россия.

Что же касается персональных устройств, IT-инфраструктур малого и среднего бизнеса, они окажутся беззащитными против квантового компьютера в случае, если он попадет в руки преступников, а тем более террористов или хакерских сетей, работающих на разведку того или иного государства. Это мало осознаваемая, но абсолютно реальная угроза подорвать безопасность, коммерцию, а главное, повседневную жизнь граждан.

Необходимость достижения квантового превосходства

Отставание в гонке за квантовыми компьютерами и квантовыми вычислениями может стать таким же опасным, как отставание в разработке новейших видов вооружения или создании «сильного» искусственного интеллекта.

Напомним, что АНБ забило тревогу в 2015 г. и прогнозировало появление возможно опасных квантовых компьютеров и

квантовых вычислений к 2030 г. Но все случилось на 10 лет раньше.

Россия располагает мощнейшим человеческим капиталом в области программирования, искусственного интеллекта и квантового компьютинга. Еще в 2019 г. для развития квантовых технологий утверждена *дорожная карта,* которая входит в национальную программу «Цифровая экономика». Карта рассчитана на срок до 2024 г. и включает три направления: вычисления, коммуникации и сенсоры.

Квантовыми вычислениями и разработкой отечественного квантового компьютера занялись в Росатоме, квантовыми коммуникациями – в РЖД, сенсорами – в Ростехе.

Ведущие российские компании сотрудничают с Росатомом в разработке квантового компьютера – Сбербанк и Сбербанк-Технологии, Газпромбанк, Газпромнефть, СИБУР и др.

Разработкой квантового компьютера в Росатоме занимаются ученые ВНИИА имени Н.Л. Духова, МГУ имени М.В. Ломоносова, МФТИ, НИТУ «МИСиС», НОЦ ФМН МГТУ имени Н.Э. Баумана, ФИАН, ряда академических институтов, а также РКЦ.

25 ноября 2020 г. объявлено о создании консорциума «Национальная квантовая лаборатория». В него вошли структура госкорпорации «Росатом» (СП «Квант»), Российский квантовый центр, Фонд «Сколково», НИУ «Высшая школа экономики», НИТУ «МИСиС», МФТИ и Физический институт имени П.Н. Лебедева.

Одновременно с созданием квантового компьютера и развитием квантовых вычислений, не дожидаясь дня Ч (так у военных обозначается день наступления войск или день нападения), в России в мобилизационном режиме необходимо развернуть работу по минимизации потенциальных рисков и угроз применения квантовых компьютеров, связанных со взломом антивирусных систем.

ВЫСТУПЛЕНИЯ НА СЕКЦИОННЫХ ЗАСЕДАНИЯХ

Секция 1.
Использование цифровых технологий в общей организации борьбы с преступностью

А.Л. Репецкая,
профессор Юридического
института Иркутского
государственного университета,
доктор юридических наук

Криптопреступления как следствие цифровизации преступности

Преступления с использованием информационно-коммуникационных технологий сегодня являются наиболее динамично развивающимися преступлениями. Ежегодный прирост так называемых киберпреступлений составляет более 70%, в 2020 г. каждое четвертое зарегистрированное преступление в общей структуре преступности (25%) совершено с использованием цифровых технологий[1].

Однако киберпреступления стремительно развиваются не только количественно. В современный период в значительной степени изменяются их структурные характеристики, связанные с развитием новых способов совершения традиционных преступлений. Эта тенденция детерминирована развитием блокчейн-технологий, появлением криптовалюты и токенов. В научной литературе преступления, совершенные с использованием криптовалюты, технологий, позволяющих ее использовать для совершения преступлений (в основном связанных с незаконным оборотом товаров и услуг), а также ее хищением, получили название крип-

[1] См.: Состояние преступности в России за январь – декабрь 2020 г. / Главный информационно-аналитический центр МВД России. М., 2021. С. 4.

топреступлений, а их совокупность стала называться криптопреступностью[1].

Криптопреступность сегодня представляет новый феномен находящейся в виртуальном пространстве преступной деятельности, посягающей на экономические, финансовые, информационные общественные отношения, и потому она занимает обособленное место в общей структуре преступности, пересекаясь с традиционными ее видами. Признаком, объединяющим разные преступления в криптопреступность, является виртуальная валюта. Она либо выступает предметом совершаемых преступлений (в основном различных видов хищений), либо используется в способах совершения ряда традиционных преступлений.

Между тем основные криминологические риски использования криптовалюты подвергались изучению лишь поверхностно. Возникновение этих рисков связано в первую очередь с огромным опозданием разработки правового регулирования использования виртуальных валют и развитием криминальных рынков товаров и услуг.

1 января 2021 г. вступил в силу Федеральный закон от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации», согласно которому сделки с криптовалютой не порождают денежных обязательств, вследствие чего она запрещена в расчетах за товары и услуги в Российской Федерации. Субъектами, имеющими право на операции с криптовалютами, являются юридические лица, имеющие лицензию на такие операции. В целом криптовалюта признана имуществом и может использоваться только для определенных целей, в рамках обеспечения ряда федеральных законов.

Иными словами, статус цифровых валют в России сегодня имеет очень ограниченные правовые рамки, они не могут быть использованы физическими лицами как легальное средство платежа, что не мешает их использованию в виде основного средства обеспечения сделок на криминальных рынках товаров и услуг.

---

[1] См.: *Долгиева М.М.* Криптопреступность как новый вид преступности: понятие, специфика // Соврем. право. 2018. № 10; *Сидоренко Э.Л.* Криптопреступность как новое криминологическое явление // О-во и право. 2018. № 2 (64).

Кроме того, ни в России, ни в мире не выработана единая оценка криптовалюты как финансового инструмента и не определены параметры безопасности ее выпуска и оборота[1] , она не признается объектом гражданских прав, используется анонимно. Все это позволяет субъектам криминальных рынков товаров и услуг не только увеличивать их обороты за счет перенесения в виртуальное пространство, но и обезопасить себя и свой криминальный бизнес, используя в расчетах цифровые валюты, обеспечивающие анонимность и продавца, и покупателя.

Виртуализация криминальных рынков запрещенных в обороте товаров (наркотиков, оружия, порнографии, персональных данных и пр.)[2], а также криминальных рынков услуг (заказные убийства, коррупционные преступления, изготовление поддельных документов, легализация преступных доходов и пр.)[3] в целом усложнила противодействие этим преступлениям. Их расследование возможно только «после подключения к сети распределительного реестра и требует специфических цифровых доказательств»[4], а фактический отказ государства от использования криптовалют в осуществлении транзанкций переместил эти финансовые инструменты в теневую сферу.

В результате криптовалюта (среди видов которой биткоин все чаще теснится с другими более анонимными виртуальными валютами, такими как Dash, Monero, ZCash [5]) превратилась в основное средство платежа в Darknet при покупке запрещенных товаров и услуг, а блокчейн-технологии позволили преступникам создавать и развивать сервисы, связанные с системами легализации преступных доходов.

---

[1] *Сидоренко Э.Л.* Указ. соч. С.15.

[2] См. подробнее о криминальном рынке товаров, запрещенных или ограниченных в обороте: *Репецкая А.Л.* Криминальный рынок: специализир. учеб. курс / Саратов. гос. акад. права; Центр по изучению организованной преступности и коррупции (Вашингтон, США). Саратов, 2007.

[3] См. подробнее о криминальном рынке услуг, запрещенных в обороте: *Репецкая А.Л.* Российский криминальный рынок услуг: структура и характеристика отдельных видов // Криминолог. журн. Байкал. гос. ун-та экономики и права. 2008. №1.

[4] *Долгиева М.М.* Указ. соч.

[5] *O`Leary R.R.* Europol Warns ZCash, Monero and Ether Playing Growing Role in Cybercrime. URL: https: //www.coindesk.com / europol warns ZCash, Monero and ether playing growing role in cybercrime.

Ярким примером виртуального криминального рынка товаров был интернет-рынок Silk Road, который реализовывал более 10 тыс. разновидностей нелегальных товаров, его общий годовой оборот превышал 17 млн долл. После пресечения деятельности этого рынка в 2014 г. вновь появившиеся криминальные рынки (в первую очередь Silk Road 2.0 и Evolution) увеличили свой доход в 10 раз[1].

В 2015–2018 гг. правоохранительные органы многих стран смогли осуществить ряд успешных операций на рынках Darknet, где продаются криминальные товары и услуги. Были разгромлены Silk Road 1.0, Silk Road 2.0, AlphaBay, Hansa. Однако на место универсальных площадок пришли специализированные рынки Darknet. По состоянию на 2018 г. наибольший оборот имели рынки, где продаются вредоносный софт и криминальные услуги, связанные с его использованием, похищенные кредитные карты, поддельные документы, оружие и педофильский контент[2].

О том, что эти рынки продолжают работу несмотря на активное противодействие им в разных странах, свидетельствует, например, арест в январе 2021 г. в Германии руководителя крупнейшей в мире нелегальной торговой площадки DarkMarket, которая насчитывала 500 тыс. пользователей и 2,4 тыс. продавцов. На этой площадке было проведено 320 тыс. транзакций. Все сделки совершались в криптовалютах, по текущему курсу ее деятельность оценена в 140 млн евро. Изъято более 20 серверов в Молдавии и на Украине[3].

Таким образом, цифровизация преступной деятельности, особенно в сфере оборота товаров и услуг, требует и цифровых средств расчетов, что влечет все большее распространение криптовалют. В результате они служат либо средством совершения преступлений, либо их предметом.

В структуру криптопреступности сегодня входит несколько групп преступлений, основным средством совершения или пред-

---

[1] *Сидоренко Э.Л.* Криптовалюта как новый юридический феномен // О-во и право. 2016. № 3(57). С. 195.

[2] *Овчинский В.С., Жданов Ю.И.* Киберполиция века: международный опыт. М.: Междунар. отношения, 2020. С.116.

[3] *Полиция* Германии ликвидировала крупнейшую в мире торговую площадку даркнета. URL: https://news.mail.ru//incident / 44857043/.

метом которых является криптовалюта. Среди доминирующих групп можно назвать незаконный оборот запрещенных законом или ограниченных в обороте товаров (наркотики и сильнодействующие вещества, оружие, порнография), преступления против собственности (в первую очередь кражи и мошенничества, где предмет преступления – криптовалюта).

Среди экономических преступлений наиболее распространенным криптопреступлением является легализация преступных доходов. Между тем это не единственное преступление в сфере экономической деятельности, которое может совершаться с использованием криптовалют. Группа деяний экономической направленности может перейти в разряд криптопреступлений при условии цифровизации предпринимательской деятельности и соответственно использовании при расчетах криптовалют, что позволит уйти от массы платежей и сборов, осуществляемых государством. Наиболее подвержены таким рискам:

преступления, совершаемые во внешнеэкономической деятельности;

налоговые преступления;

банкротство при аналогичных условиях;

преступления, связанные с нарушением валютного законодательства, когда платежи по договорам перечисляются в виртуальной валюте и т.п.

Следует отметить, что если анализ распространенных групп криптопреступлений в целом представлен в научной литературе, то состояние и развитие преступлений в экономической сфере оценить сложно, поскольку отсутствует определение правового статуса криптовалют и признание их объектом гражданских прав. По этой же причине легализация преступных доходов с использованием блокчейн-технологий становится все более популярной: отсутствие правовой регламентации не позволяло признать совершенные с криптовалютой сделки преступными. Соответственно, уровень данного вида легализации рос колоссальными темпами. Так, если в 2015 г. количество зарегистрированных фактов использования виртуальной валюты для отмывания преступных доходов не превышало 5% от общего объема криптопреступлений, то в 2018 г. этот показатель превысил 40%[1]. Вряд ли

[1] *O`Leary R.R.* Europol Warns ZCash, Monero and Ether Playing Growing Role in Cybercrime.

отказ государства от признания цифровых валют средством платежа повлияет на улучшение ситуации с легализацией преступных доходов.

Анализ детерминации распространения криминальных рынков в интернет-сетях свидетельствует, что одним из основных условий их развития выступает анонимный характер расчетов при использовании криптовалют, т.е. отсутствие идентификации пользователей. Это позволяет осуществлять оборот наркотических средств, незаконного контента и прочих запрещенных товаров и услуг без опасения быть обнаруженным.

Так, по данным TOR Metrics, Россия занимает второе место в мире после США по числу пользователей теневого Интернета в секторе продажи наркотиков[1]. Исследователями отмечается, что криптонаркотизм уже перешел на этап формирования собственной инфраструктуры и криминальной специализации[2]. Это в свою очередь влечет трансформацию криминальных профессий и качественные изменения в профессиональной преступности.

Что касается преступлений против собственности, совершаемых в виртуальном пространстве, то ущерб от них растет беспрецедентными темпами в среднем на 300% в год[3]. Поскольку виртуальное пространство не имеет границ, от хищений криптовалюты страдают пользователи во всем мире.

Отдельное место в криптовалютной преступности занимают преступления террористического характера. Финансирование терроризма и экстремизма с использованием криптовалюты в значительной степени облегчает и ускоряет доступ преступников к оружию, технике, средствам передвижения, документам; обеспечивает наем боевиков и прочие необходимые для их деятельности затраты. При этом отследить поступление средств и приобретение на них товаров и услуг не представляется возможным, так как все транзакции происходят в теневом секторе Интернета.

Угрозу представляет и использование криптовалюты для оплаты коррупционных услуг. Опасность разоблачения должностных лиц, оказывающих коррупционные услуги, фактически отсутствует. Электронный кошелек, в который поступают сред-

---

[1] URL: https://metrics.torproject.org/bandwidth.html.
[2] *Сидоренко Э.Л.* Криптопреступность как новое криминологическое явление. С. 18.
[3] Там же.

ства от неидентифицированного пользователя, покупающего такую услугу, и пароль, известный только владельцу, также обеспечивают безопасность преступной деятельности. Представляется, что тренд на виртуализацию коррупционных услуг является реальностью ближайшего будущего.

Угрозы национальной безопасности со стороны криптопреступности в ряде стран оцениваются так высоко, что в 2018 г. был создан специальный альянс, который получил название J5. В него входят Австралийская комиссия по преступности (ACIC), Австралийское налоговое управление (ATO), Канадское налоговое агентство (CRA), Служба расследования налоговых преступлений Нидерландов (FIOD), Управление Ее Величества по налогам и таможенным пошлинам (HMRC) и Отдел криминальных расследований Налогового управления США (IRS-CI). Таким образом, США, Австралия, Канада, Нидерланды и Великобритания будут вместе пресекать отмывание денег, финансирование терроризма и незаконное обогащение, связанное с криптовалютами[1]. В Индии для расследования криптовалютных преступлений было создано специальное криптоподразделение национальной киберкриминалистической лаборатории (NCFL), которое названо Cypad[2].

В целом стоит констатировать, что с развитием цифровизации общественной жизни ускорится переход различных видов преступной деятельности корыстного характера в виртуальную сферу. Использование криптовалют при этом ускоряет и облегчает получение прибыли от различных видов преступного бизнеса, других преступлений и обеспечивает безопасность субъектам.

Правоохранительные органы вынуждены будут приспосабливаться, менять методики выявления и расследования преступлений, как полностью, так и частично совершаемых в киберпространстве. Это может изменить подходы к процессу подготовки кадров для правоохранительной системы, изменить деятельность системы уголовной юстиции.

---

[1] URL: https:// news4auto.ru/piat-stran-sozdali-j5-alians-protiv-kriptoprestyplenii/.
[2] URL: https:// www.thenhindu.com/news/cities/Delhi/article26307171.ece/.

Е.В. Рогова,
профессор кафедры
Иркутского юридического
института (филиала)
Университета прокуратуры
Российской Федерации,
доктор юридических наук, доцент

Роль информационно-коммуникационных технологий и компьютерной информации в совершении корыстных преступлений

В современных условиях происходит становление цифровой экономики. Это неизбежный процесс внедрения передовых достижений в области информационно-коммуникационных технологий и компьютерной информации, обусловленный тем обстоятельством, что такая экономика является наиболее эффективной и конкурентоспособной. Цифровая экономика позволяет хозяйствующим субъектам оптимизировать различные процессы, связанные с производством товаров и оказанием услуг.

Однако, как справедливо отмечается в юридической литературе, стремительная цифровизация и глобализация, расширение информационного пространства помимо положительных моментов имеют и негативную сторону, состоящую в уязвимости сферы информационно-коммуникационных технологий и компьютерной информации, которую активно используют преступники в своих корыстных целях[1].

Статистические показатели и исследования корыстной преступности свидетельствуют о том, что данный вид преступности занимает лидирующие позиции как в России, так и в зарубежных странах. А разнообразной эту преступность можно назвать потому, что к ней можно отнести квартирные, карманные кражи, коррупционные преступления, присвоение и растрату, мошенниче-

[1] *Русскевич Е.А., Фролов М.Д.* Мошенничество в сфере компьютерной информации: монография. М., 2020. С. 4–5; *Ефремова М.А.* Уголовная ответственность за преступления, совершаемые с использованием информационно–телекоммуникационных технологий: монография. М., 2015. С. 7–9.

ство, рейдерские захваты, незаконную торговлю оружием, наркотиками, бандитизм, торговлю людьми и т.п.

Как уже отмечалось, в условиях глобального развития информационно-коммуникационных технологий и компьютерной информации преступники переходят в онлайн-среду, создавая новые схемы совершения преступлений. На официальном сайте МВД России приводятся примеры распространенных в настоящее время видов мошенничества, совершаемых в онлайн-среде, начиная от так называемых брачных мошенничеств, заканчивая историями о помощи больным детям и т.п.[1]

Возрастает количество мошенничеств, краж с использованием электронных средств платежа, распространение получают факты так называемого телефонного хищения. Так, на сайте Сбербанка России приводятся предостережения от телефонных краж, мошенничеств, совершаемых различными способами. Например, преступник, звоня по телефону, представляется сотрудником службы безопасности банка и просит сообщить данные карты, или так называемый перевод по ошибке, когда лицу приходит SMS-сообщение, подделанное под банковское, о якобы перечисленных денежных средствах на его счет, следом приходит сообщение с просьбой вернуть «ошибочно переведенные» средства. Еще один вариант такого мошенничества заключается в предложении со стороны преступников «выгодных инвестиций», при котором потерпевшему предлагается осуществить выгодное вложение денежных средств путем перевода этих средств на счет злоумышленника. Также можно отметить «выигрыши в лотереях», проведение «опросов от Сбербанка» и т.п.[2]

Распространение получает такой способ совершения хищения, при котором преступники обзванивают людей под видом сотрудников туристических компаний, авиакомпаний и предлагают оформить возврат потраченных на приобретение путевок или билетов средств. Потерпевшие в ряде случаев, не задумываясь, называют данные банковских карт, в результате чего происходят списания с их банковских счетов. Некоторые преступники предлагают полу-

---

[1] *Распространенные* виды мошенничества с использованием компьютерных технологий. URL: https://мвд.рф/document/11700239 (дата обращения: 02.02.2021).

[2] *Как* обманывают мошенники. URL: https://www.sberbank.ru/ru/person/dist_services/cybersecurity/cybersecurity_situations (дата обращения: 02.02.2021).

чить социальные выплаты и материальную помощь, собирая информацию о банковских картах и персональные данные.

Увеличивается количество мошенничеств в сфере компьютерной информации. Компьютерными мошенниками создаются сайты-двойники для списания денежных средств потерпевших с их банковских счетов, взламываются аккаунты в социальных сетях и т.п. Примером может служить создание сайтов-одностраничников, где выкладываются товары, визуально схожие с брендовыми, но отличающиеся по ценам. С учетом цены ниже рыночной такие сайты работают по стопроцентной предоплате. По договоренности с продавцом деньги перечисляются, после чего псевдопродавец исчезает. Зеркальные сайты создаются по доставке продуктов, медикаментов и т.п.

Исходя из изложенного, можно прийти к выводу о том, что высокая скорость развития информационных технологий требует динамичности уголовного законодательства, которое должно отражать изменения общественных отношений в условиях цифровой глобализации, появления новых способов совершения преступлений. Традиционный механизм уголовно-правовой охраны в настоящее время не в полной мере срабатывает в условиях изменяющейся преступности по причине цифровой трансформации. Вопрос об адаптации уголовного закона к новым условиям и актуальным запросам информационного общества является одним из первоочередных. Создание адекватной правовой базы, регулирующей вопросы противодействия преступности, в условиях научно-технического прогресса является одной из гарантий обеспечения национальной безопасности[1].

В контексте рассматриваемых проблем интерес представляет мошенничество в сфере компьютерной информации, ответственность за которое предусмотрена ст. 159^6 УК РФ. Анализ уголовно-правовой нормы и практики ее применения свидетельствует о несовершенстве статьи. Сложности в толковании указанной нормы начинаются с определения объекта и предмета. Среди ученых нет единства взглядов относительно данных элементов состава преступления. Распространенной точкой зрения

[1] *Козаев Н.Ш.* Современные технологии и проблемы уголовного права (анализ зарубежного и российского законодательства): монография. М., 2015. С. 7.

исходя из расположения рассматриваемой нормы в гл. 21 УК РФ (Преступления против собственности) является понимание объекта преступления, предусмотренного ст. 159^6 УК РФ, как общественных отношений в сфере собственности[1]. Вместе с тем, по мнению В.И. Гладких, «чрезвычайно сложно определить объект и предмет преступления, предусмотренного ст. 159^6 УК РФ, поскольку сфера компьютерной информации относится к другой сфере общественных отношений». На основании изложенного автор приходит к выводу о некорректном расположении ст. 159^6 в структуре Особенной части УК РФ[2]. Некоторые авторы говорят о наличии двух объектов в рассматриваемом составе преступления. Основным объектом являются общественные отношения в сфере собственности, дополнительным – общественные отношения в сфере безопасности компьютерных систем[3] или общественные отношения в сфере компьютерной информации[4]. Ведутся дискуссии и относительно объективной стороны рассматриваемого состава преступления.

Следует также отметить, что в гл. 21 УК РФ закреплены нормы, устанавливающие уголовную ответственность за мошенничество с использованием электронных средств платежа (ст. 159^3), за кражу с банковского счета, а равно в отношении электронных денежных средств (п. «г» ч. 3 ст. 158).

В правоприменительной практике нередко возникает вопрос, по какой из указанных норм квалифицировать противоправное деяние. В частности, это касается, например, хищений денежных средств с чужого банковского счета с использованием услуги Мобильный банк Сбербанка России. Абоненту ошибочно подключается услуга Мобильный банк с информацией о денежных средствах, принадлежащих другому лицу, предоставляющая

---

[1] *Комментарий* к Уголовному кодексу Российской Федерации (науч.-практ., постат.) / под ред. проф. С.В. Дьякова, проф. Н.Г. Кадникова. М., 2015. С. 406.

[2] *Гладких В.И.* Компьютерное мошенничество: а были ли основания его криминализации? // Рос. следователь. 2014. № 22.

[3] *Сафонов О.М.* Уголовно-правовая оценка использования компьютерных технологий при совершении преступлений: состояние законодательства и правоприменительной практики, перспективы совершенствования: дис. … канд. юрид. наук. М., 2015. С. 115–116; *Третьяк М.И.* Мошенничество как преступление против собственности в современном уголовном праве: курс лекций. М., 2014. С. 174; и др.

[4] *Лопатина Т.М.* Проблемы формирования уголовно-правового способа борьбы с компьютерным мошенничеством // Б-ка криминалиста. 2013. № 5. С. 38.

право распоряжаться денежными средствами, находящимися на его расчетном счете. Виновные пользуются такими ошибочными подключениями и переводят деньги на свои счета или на счета сим-карт своих мобильных телефонов. В одних случаях такие действия квалифицируются как мошенничество в сфере компьютерной информации, в других – как кража. Возникает вопрос, почему судами принимаются разные решения. Ответ состоит в том, что недостаточно понятны формулировки законодателя, не совсем понятно, какие деяния образуют объективную сторону преступления, предусмотренного ст. 159^6 УК РФ. Исходя из анализа диспозиции указанной нормы можно сделать вывод о том, что это особый вид мошенничества, не вписывающийся в классическое понимание мошенничества как формы хищения путем обмана (пассивного или активного) физического лица.

На практике возникают вопросы и при квалификации ситуаций, связанных с использованием чужой банковской карты в магазине вопреки волеизъявлению владельца карты. В некоторых случаях суды квалифицируют такие противоправные деяния как мошенничество с использованием электронных средств платежа, а в других случаях – как кражу с банковского счета, а равно в отношении электронных денежных средств[1].

Развивающиеся общественные отношения, связанные с внедрением информационно-коммуникационных технологий и компьютерной информации во все сферы жизнедеятельности человека, в том числе и в экономическую сферу, а также вопросы, возникающие в правоприменительной практике при квалификации корыстных преступлений, совершаемых с использованием указанных технологий, обусловливают совершенствование уголовного законодательства в этой части. Одним из таких решений, направленных на совершенствование российского уголовного закона, может стать установление уголовной ответственности за хищение с использованием информационно-коммуникационных технологий и компьютерной информации в рамках самостоятельного состава преступления. В связи с этим интересен опыт, в

[1] Определение Судебной коллегии по уголовным делам Верховного Суда РФ от 29.09.2020 № 12-УДП20-5-К6. URL: https://ukrfkod.ru/pract/opredelenie-sudebnoi-kollegii-po-ugolovnym-delam-verkhovnogo-suda-rossiiskoi-federatsii-ot-29092020-n-12-udp20-5-k6/ (дата обращения: 02.02.2021).

частности стран СНГ, в уголовном законодательстве которых есть уголовная ответственность за хищение путем использования компьютерной техники (ст. 212 УК Республики Беларусь, ст. 181 УК Республики Армения).

О.Н. Тисен,
начальник Юридического
управления Федеральной службы
по финансовому мониторингу,
доктор юридических наук

Доказывание преступлений, связанных с финансированием терроризма

В последнее время деятельность правоохранительных органов по выявлению фактов финансирования терроризма существенно активизировалась. Так, в 2019 г. выявлено 169 фактов финансирования терроризма, что на 60% больше, чем в предыдущем году (103), в 2020 г. – 151.

Вместе с тем количество установленных случаев финансирования террористической деятельности незначительно в сравнении с масштабами анализируемых преступлений и ежегодно не превышает 9% в общей структуре террористической преступности в стране.

Так, из 2342 преступлений террористической направленности, зарегистрированных в 2020 г., по факту финансирования терроризма возбуждено лишь 151 уголовное дело (или 6,4%), в 2019 г. – 169 из 1806 (9%), в 2018 г. – 103 из 1679 (6,1%), в 2017 г. – 119 из 1871 (6,3%), в 2016 г. – 53 из 2227 (2,3%), в 2015 г. – 38 из 1538 уголовных дел (2,4%).

В следственной практике отсутствует единая позиция в части особенностей применения ст. 205^1 УК РФ. Наибольшие трудности возникают при доказывании умысла на финансирование терроризма и его квалификации.

В результате проведенного нами анализа приговоров по уголовным делам о преступлениях, предусмотренных ст. 205^1 и

ч. 1 ст. 208 УК РФ, постановленных судами в период с 2013 г. по первое полугодие 2020 г., а также позиции Верховного Суда Российской Федерации, отраженной в апелляционных определениях, установлено, что уголовно наказуемым в Российской Федерации является предоставление средств:

для подготовки и совершения преступлений террористической направленности, предусмотренных ст. 205, 205^1, 205^2, 205^3, 205^4, 205^5, 206, 208, 211, 220, 221, 277, 278, 279 и 361 УК РФ;

незаконному вооруженному формированию, террористической организации и сообществу как на цели, связанные с совершением преступлений террористической направленности, так и для обеспечения их функционирования: на продукты питания, одежду, жилье, медикаменты, транспортные услуги и т.д.;

лицу, заведомо для фигуранта участвующему в незаконном вооруженном формировании, террористической организации и сообществе, как на цели, связанные с совершением преступлений террористической направленности, так и для обеспечения его жизнедеятельности, при осознании того, что эти средства могут быть использованы как на продукты питания, одежду, жилье, медикаменты, транспортные услуги, лечение и т.д., так и на приобретение обмундирования, оружия, боеприпасов и совершение преступлений террористической направленности;

лицу, заведомо для фигуранта причастному к террористической деятельности, но не являющемуся участником НВФ, МТО или ТС, при осознании того, что эти средства могут быть использованы как на личные нужды, так и для совершения преступлений террористической направленности;

для оплаты транспортных расходов на проезд к месту участия в террористической деятельности (например, покупка авиабилета в Турцию для последующего прибытия в Сирию либо предоставление средств для этих целей).

Основополагающей особенностью доказывания преступлений, связанных с финансированием терроризма, является необходимость установления осведомленности лица, предоставившего средства, о том, что они предназначены лицам, причастным к терроризму, и могут быть использованы ими как на личные нужды, так и на совершение преступлений террористической направленности либо функциональное обеспечение НВФ/МТО.

Состав преступления образует предоставление средств не только на совершение преступлений террористической направленности, но и на финансирование лица или организации, заведомо для субъекта причастных к террористической деятельности.

Признавая подсудимых виновными в финансировании терроризма, суды указывают, что они оказывали материальную поддержку НВФ или МТО, осознавая, что деятельность этих организаций направлена на совершение преступлений террористической направленности[1]. Такие действия суды рассматривают как умышленные, поскольку, «предоставляя денежные средства и иное имущество участникам МТО, лицо, безусловно, должно осознавать, что они могли быть использованы полностью или частично для совершения преступлений террористической направленности»[2].

В апелляционном определении от 28.08.2019 № 205-АПУ19-22 Судебная коллегия по делам военнослужащих Верховного Суда Российской Федерации указала, что в силу требований уголовного законодательства финансирование терроризма является оконченным преступлением с момента предоставления или сбора средств либо оказания финансовых услуг с осознанием того, что они предназначены для финансирования организации, подготовки или совершения хотя бы одного из преступлений, приведенных в ст. 205[1] УК РФ, а выяснение вопроса о том, как террористы распорядились полученными средствами, в предмет доказывания по уголовному делу не входит.

В апелляционном определении от 05.12.2019 № 224-АПУ19-11 Судебная коллегия по делам военнослужащих Верховного Суда Российской Федерации указала, что довод о том, что по делу не установлена причастность осужденных за финансирование терроризма к подготовке либо совершению одного из преступлений, предусмотренных примечанием к ст. 205[1] УК РФ, является несостоятельным, поскольку определяющим для установления факта совершения преступления, предусмотренного ч. 4

---

[1] Апелляционное определение Судебной коллегии по делам военнослужащих Верховного Суда РФ от 19.03.2019 № 201-АПУ19-3.

[2] Приговор Северо-Кавказского окружного военного суда от 18.12.2017 в отношении А., признанного виновным в совершении трех преступлений, предусмотренных ч. 1 ст. 205[1] УК РФ.

ст. 205^1 УК РФ, является подтверждение совокупностью собранных доказательств осознания осужденным того, что средства, сбор и перечисление которых он организовал, предназначены для финансирования организации, подготовки или совершения хотя бы одного из преступлений, предусмотренных ст. 205, 205^1, 205^2, 205^3, 205^4, 205^5, 206, 208, 211, 220, 221, 277, 278, 279 и 360 УК РФ, либо для финансирования или иного материального обеспечения лица в целях совершения им хотя бы одного из этих преступлений, либо для обеспечения организованной группы, незаконного вооруженного формирования, преступного сообщества (преступной организации), созданных или создаваемых для совершения хотя бы одного из указанных преступлений.

Также не влияет на уголовно-правовую оценку отсутствие сведений о личном получении перечисленных на территорию другого государства денежных средств конкретными участниками НВФ или МТО, которым они предназначались, с использованием банковских карт, держателями которых они являются.

В апелляционном определении от 22.10.2019 № 208-АПУ19-10 Судебная коллегия по делам военнослужащих Верховного Суда Российской Федерации отметила, что то обстоятельство, что осужденный за финансирование терроризма не был знаком с получателями денежных переводов, не имеет правового значения для дела, поскольку по смыслу ст. 205^1 УК РФ финансированием терроризма следует признавать в том числе предоставление или сбор денежных средств с осознанием того, что они предназначены для финансирования террористической организации.

Сумма финансирования не влияет на квалификацию преступления, предусмотренного ст. 205^1 УК РФ[1].

Для признания лица виновным в финансировании терроризма наличие обвинительного приговора в совершении преступлений террористической направленности в отношении получателя средств не требуется, о чем неоднократно указывали суды в приговорах. Вместе с тем в случае обвинения фигуранта в финансировании конкретного лица в материалах уголовного дела должны быть сведения о его причастности к террористической деятельно-

[1] Приговор Северо-Кавказского окружного военного суда от 08.08.2018 в отношении Н., признанного виновным в совершении преступления, предусмотренного ч. 1 ст. 205^1 УК РФ.

сти: постановления о возбуждении уголовного дела, о привлечении в качестве обвиняемого, об объявлении в розыск, о приостановлении предварительного следствия и т.д.[1]

Следует учитывать, что уголовной ответственности по российскому законодательству подлежат в том числе российские граждане, осуществившие финансирование других лиц в целях осуществления ими террористической деятельности, в период нахождения ими за пределами территории Российской Федерации.

Л.В. Яковлева,
главный научный сотрудник
ВНИИ МВД России,
доктор юридических наук, доцент

Проблемы криминализации новых видов общественно опасных деяний, совершаемых с использованием информационно-телекоммуникационной сети «Интернет»

Среди информационно-телекоммуникационных сетей сеть «Интернет» занимает ведущее положение. Согласно данным агентств We Are Social и Hootsuite, по состоянию на январь 2021 г. 59,5% населения планеты используют сеть «Интернет», аудитория социальных сетей достигает 53,0%[2]. Для Российской Федерации эти показатели составляют соответственно 85 и 67,8%[3]. Даже учитывая погрешности в результатах и оговорки авторов относительно методики сбора данных, следует признать, что ежегодно число людей, не знакомых с сетью «Интернет», уменьшается, а число его пользователей неуклонно растет.

---

[1] Апелляционное определение Судебной коллегии по делам военнослужащих Верховного Суда РФ от 05.12.2019 № 224-АПУ19-11.

[2] *Кейп С.* Глобальный обзорный отчет цифровых технологий 2021 (январь 2021) // Глобальные отчеты. 2021. URL: https://datareportal.com/reports/digital-2021-global-overview-report (дата обращения: 16.02.2021).

[3] *Кейп С.* Цифровые технологии 2021: Российская Федерация (январь 2021) // Местные отчеты. 2021. URL: https://datareportal.com/reports/digital-2021-russian-federation (дата обращения: 16.02.2021).

Столь масштабное проникновение сети в жизнь общества не могло не отразиться на показателях количества преступлений, совершаемых с использованием ее возможностей. Ответом законодателя стала криминализация деяний, совершаемых с помощью современных достижений технического прогресса в области информационных технологий.

Действующий УК РФ содержит около 20 составов преступлений, которые совершаются с использованием сети «Интернет». Они включены в разные главы кодекса, посягают на различные охраняемые законом объекты. Это и личность, и интересы семьи и несовершеннолетних, и общественная нравственность, и общественная безопасность, и экологические преступления, и преступления в сфере экономики, и преступления экстремистской направленности.

Как правило, способ совершения преступления, предусматривающий использование сети «Интернет», закрепляется в квалифицированных составах. Однако в ряде деяний он включен в основной состав. Вместе с тем уголовное законодательство меняется вслед за изменениями, происходящими в жизни общества, поэтому определить исчерпывающий перечень преступлений, которые могут совершаться таким способом, невозможно. Во избежание внесения постоянных дополнений в УК РФ предлагалось включить признак «совершение преступления с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет» в качестве отягчающего обстоятельства в ст. 63 УК РФ[1].

Такое решение позволит оперативно реагировать на случаи совершения уже закрепленных в УК РФ преступлений новым способом – с использованием сети «Интернет», квалифицируя деяния с учетом всех фактических обстоятельств. Но до сих пор это предложение не реализовано, и законодатель идет по пути дифференциации ответственности в рамках соответствующих статей УК РФ. Только в течение нескольких лет данный признак был включен в ст. 238^1 (ч. 1^1), ст. 158 (п. «г» ч. 3) УК РФ, а также предусмотрен в ряде введенных в УК РФ статей (110^1, 110^2 151^2).

---

[1] *Добрикова Е.* Использование Интернета при совершении преступлений предлагают отнести к отягчающим обстоятельствам. URL: https://www.garant.ru/news/722335/ (дата обращения: 20.01.2021).

Между тем в последнее время появились новые виды противоправных действий, совершить которые невозможно без использования сети «Интернет». К преступлениям, в частности, предлагают отнести так называемый треш-стрим, в котором демонстрируются сцены насилия, унижения человеческого достоинства и пр. Подобные трансляции не подпадают под действие ни одной статьи УК РФ. Уголовно наказуемы только насильственные действия, совершаемые в отношении жертв этих трансляций.

Вопрос о необходимости установления уголовной ответственности за треш-стрим обсуждается в Совете Федерации. Повышенный интерес к этой проблеме обусловлен случаями смерти во время демонстрации в сети сюжетов с издевательствами над людьми[1], самым известным из которых стал случай с видеоблогером С. Решетниковым, в результате действий которого погибла девушка[2].

В переводе с английского языка trash stream буквально означает мусорный поток. Как социальное явление треш-стрим представляет собой трансляцию в сети «Интернет» в режиме реального времени разного рода насильственных действий, сопряженных с глумлением и издевательствами над человеком. Жертвы, как правило, соглашаются участвовать в подобных «действах» добровольно за материальное вознаграждение. Организаторы видеосъемок, а также лица, непосредственно применяющие насилие, стремятся к извлечению из таких трансляций выгоды в виде перечисляемых зрителями денежных средств либо к поднятию рейтинга своих видеоблогов. Нередко в роли организатора и исполнителя выступает одно лицо.

Председатель временной комиссии Совета Федерации по информационной политике и взаимодействию со средствами массовой информации А.К. Пушков предлагает дополнить ст. 282 УК РФ частью, предусматривающей ответственность за совершение публично с использованием сети «Интернет» действий, уни-

---

[1] *Россиянин* умер в прямом эфире треш-стрима // LENTA.RU: Интернет и СМИ. 2021. URL: https://lenta.ru/news/2021/01/28/efir/?utm_source=24smi&utm_medium=exchange&utm_term=14111&utm_content = 3302875&utm_campaign=12675&es=24smi (дата обращения: 28.01.2021).

[2] *Козлова Н.* Добивал в прямом эфире // Рос. газ. 2020. 6 дек. Федеральный выпуск № 275 (8329).

жающих или умаляющих человеческое достоинство, которые сопровождаются применением насилия или угрозой его применения. Демонстрироваться такие действия могут как в режиме реального времени, так и в видеозаписи. Преступными они будут признаваться в случаях, когда преследуют цель извлечения материальной или иной выгоды.

Представляется, что предложение об установлении уголовной ответственности за треш-стрим заслуживает поддержки. В обществе, особенно в молодежной среде, всегда найдутся лица, готовые ради обретения известности совершать аморальные, а подчас противозаконные поступки и демонстрировать их через сеть «Интернет», тем более если эти действия одобряет аудитория, выражая одобрение и поддержку лайками или перечислением денежных средств за просмотр. Предотвратить широкое распространение подобного рода видеосюжетов могут информационно-телекоммуникационные сети, оперативно блокируя трансляцию действий соответствующего содержания. Однако этих мер может оказаться недостаточно, поскольку молодежные субкультуры появляются и развиваются по своим законам, а влияние сети на них, как отмечается в ряде исследований, огромно[1].

Детально исследуя феномен треш-стрима, причины его появления, Е. Смирнова приходит к выводу, что существующие в обществе социальные проблемы, решить которые молодежь самостоятельно не может, бездуховность приводят к тому, что насилие становится товаром, продаваемым и приобретаемым через Интернет[2].

Противники криминализации треш-стрима в качестве оправдания их существования и свободного распространения ссылаются на то, что в художественных и документальных фильмах демонстрируются и сцены насилия, и убийства. Такого рода аргументы в отношении рассматриваемого социального явления несостоятельны. Критерием разграничения треш-стримов и произведений искусства служит цель их создания, а разница в целях показа насилия в произведениях искусства и в бытовых видео из

---

[1] *Суходольская Ю.В.* Субкультуризация массового убийства в образовательных организациях как новый российский криминологический феномен // Законность. 2020. № 10. С. 38.

[2] *Смирнова Е.* Треш-стрим как образ жизни // Эксперт. 2020. № 51 (1189).

реальной жизни их авторов значительная. В произведениях искусства насилие всегда осуждается, пропагандируются идеи добра, проводится мысль о неотвратимости наказания. Бытовые видео, демонстрирующие сцены насилия или унижения людей, снимают, как указывалось, с иными целями – приобрести материальную выгоду или прославиться в сети.

Вместе с тем сформулированная А.К. Пушковым новая часть ст. 282 УК РФ нуждается в корректировке, как и предложение о включении ее именно в данную статью.

Деяния, закрепленные в ст. 282 УК РФ, относятся к числу экстремистских. Их основная цель – возбудить ненависть или вражду либо унизить человеческое достоинство лиц, относящихся к другому полу, расе, национальности, говорящих на ином языке, исповедующих иную религию и т.д. Для организаторов треш-стримов перечисленные обстоятельства не важны. Они преследуют корыстные или иные низменные цели.

Демонстрируемые сцены насилия или унижения людей противоречат нравственным устоям общества, являются аморальными. Соответственно объектом такого рода посягательств является общественная нравственность как регулятор поведения человека в обществе, а не основы конституционного строя.

Кроме того, треш-стримы нельзя рассматривать как «действия, содержащие унижение человеческого достоинства с применением или с угрозой применения насилия, физических издевательств, оскорблений и других форм хулиганского поведения, умаляющего достоинство личности»[1]. Фактически они представляют собой трансляцию совершения насильственных преступлений, ответственность за которые закреплена в статьях гл. 16 УК РФ (умышленное причинение вреда здоровью различной тяжести, побои, истязания и пр.).

Таким образом, если вводить новую норму в УК РФ, то в гл. 25 (Преступления против здоровья населения и общественной нравственности), дополнив ее, например, ст. 239[1]. Под уголовный запрет должны подпадать не насильственные действия, а трансляция с использованием сети «Интернет» сцен насилия, глумления над человеком.

---

[1] *Роскомнадзор* поддержал введение уголовной ответственности для организаторов треш-стримов // ТАСС. 2021. URL: https://tass.ru/obschestvo/10513357 (дата обращения: 23.01.2021).

С.А. Алтухов,
профессор кафедры уголовного права и криминологии Ростовского института (филиала) Всероссийского государственного университета юстиции (РПА Минюста России), кандидат юридических наук, доцент

Проблемы борьбы с преступностью в условиях изменения формата медиапространства

Обращение к теме противодействия преступности в условиях разрастания новых угроз неслучайно. Затяжной социально-экономический кризис, деструктивная геостратегия США и западных партнеров с их санкционным давлением и агрессивной антироссийской риторикой, а также новые конфронтации политического характера внутри страны со всей очевидностью должны предопределять рост преступности и изменение ее качественных характеристик.

Вместе с тем на фоне замедления темпов развития экономики, снижения уровня доходов населения[1], роста числа безработных[2], некомплекта кадров в правоохранительных органах (в МВД – до 7,5%)[3], психологической усталости и напряжения сотрудников в ожидании очередного этапа реформирования системы государственных органов преступность в стране продолжает снижаться. За последние годы статистически она даже стабилизировалась. Так, количество зарегистрированных преступлений в 2020 г. выросло всего на 1%, превысив прошлогодний показатель на 20 тыс. преступлений, достигнув отметки в 2044,2 тыс.[4]

---

[1] *Экономисты* оценили снижение реальных доходов населения из-за карантина. Падение может стать максимальным с 2014 года. URL: https://www.rbc.ru/economics/06/04/2020/5e8732e89a79470b55b42d72 (дата обращения: 18.01.2021).

[2] *Леконцев И.П.* Бедность в России: официальная статистика и результаты социологических опросов ВЦИОМ // Мониторинг общественного мнения: экономические и социальные перемены. 2016. № 2.

[3] *Колокольцев* заявил об усилении дефицита аттестованных кадров в МВД. URL: https://ria.ru/20200226/1565231175.html (дата обращения: 18.01.2021).

[4] Состояние преступности в Российской Федерации за январь – декабрь 2020 года. URL: https://мвд.рф/reports/item/22678184/ (дата обращения: 18.01.2021).

Указанные в итоговом отчете МВД России данные о состоянии и принятых мерах по противодействию преступности за 2020 г., в особенности о заметном сокращении количества ряда преступлений, следует оценивать с известной долей условности. Так, вряд ли стоит уповать на повышение уровня безопасности даже при снижении количества зарегистрированных убийств, когда десятки тысяч лиц, пропавших без вести, так и остаются ненайденными. Например, за 2019 г. удалось установить лишь 30,9% безвестно отсутствующих граждан от общего числа разыскиваемых. А ведь более 30,5 тыс. человек так и остались без вести пропавшими[1].

Нельзя не заметить и другие тревожные тенденции. Удельный вес лиц, ранее совершавших преступления, подошел к 60%, а доля ранее судимых – к 30%. Наблюдается рост количества преступлений экономической и коррупционной направленности (в особенности в сфере экономической деятельности), причиненного такими преступлениями ущерба. Так, размер ущерба от преступлений экономической направленности в 2020 г. только по расследованным делам составил 394,5 млрд руб., что больше прошлогоднего показателя на 13,6%. Набирает силу и организованная преступная деятельность (+8,8%).

Однако настоящей бедой стали преступления, совершенные с использованием информационно-коммуникационных технологий. В 2020 г. они составили четвертую часть всех зарегистрированных преступлений, а их количество в абсолютном выражении выросло более чем на 73% по сравнению с 2019 г. Более половины таких преступлений относятся к категории тяжких и особо тяжких (52,3%), причем их количество за год увеличилось почти вдвое (+87,5%), а практически половину из них составили мошеннические действия (46,3%).

Представляется, что подобного рода «эффект» стабилизации и даже снижения преступности, который наблюдался и ранее (например, в период августовского путча 1991 г.), можно объяснить рядом объективных и субъективных факторов: 1) деструктивным психологическим ожиданием населением новых небла-

[1] *Обеспечение* общественного порядка и противодействие преступности: уточненный годовой отчет о ходе реализации и оценке эффективности государственной программы за 2019 год. М.: МВД России, 2020. С. 4.

гоприятных последствий, в том числе связанных с распространением пандемии коронавируса; 2) снижением уровня доверия к государственным органам и должностным лицам на фоне роста коррупционных скандалов с их участием, необоснованных, а нередко и незаконных решений следственных и судебных органов; 3) сокрытием объективных сведений об изменениях криминологической ситуации, вызванных продолжающейся конфронтацией между правоохранительными органами и попытками искусственного занижения показателей преступности[1]; 4) отсутствием реальных возможностей реагирования на криминальные проявления, в особенности на преступления небольшой и средней тяжести. Так, при наличии многочисленных вакансий в службе участковых уполномоченных полиции[2] они продолжают нести службу за пределами своих физических возможностей[3]. Столь высокий коэффициент полезного действия сотрудников можно сравнить с виртуальной реальностью и появлением киберполиции[4].

Изменившийся формат практически всех правоотношений (включая и отношения на межгосударственном уровне) во многом обусловлен наметившейся тенденцией глобального пересмотра традиционных ценностей и способов их достижения. Одним из таких способов можно признать использование информационных технологий, которые заполняют информационное пространство нередко низкопробной, ложной, необъективной, аморальной, безнравственной и порой циничной продукцией, о чем стали упоминать и высокопоставленные чиновники[5]. Такой про-

---

[1] В системе МВД России начиная с 2015 г. перестали публиковать данные о количестве заявлений и сообщений о происшествиях.

[2] *В МВД* назвали число вакантных должностей участковых. URL: https://news.rambler.ru/other/43395659/?utm_content=news_media&utm_medium=read_more&utm_source=copylink (дата обращения: 18.01.2021).

[3] Участковые уполномоченные полиции с учетом представленных результатов деятельности указанной службы только в 2019 г. рассмотрели более 13,6 млн заявлений и сообщений граждан. Каждый сотрудник в среднем ежедневно рассматривал как минимум один материал, зарегистрированный в книге учета сообщений о происшествиях (КУСП), и осуществлял около 70 профилактических мероприятий с потенциальными правонарушителями, в том числе ранее привлекавшимися к уголовной ответственности.

[4] *Жданов Ю.Н., Овчинский В.С.* Киберполиция XXI века: международный опыт. М.: Междунар. отношения, 2020. С. 16.

[5] *Кудрин* раскритиковал российские телевизионные ток-шоу. URL: https://www.mk.ru/politics/2021/01/15/kudrin-raskritikoval-rossiyskie-televizionnye-tokshou.html?utm_referrer=https%3A%2F%2Fzen.yandex.com (дата обращения: 18.01.2021).

цесс изменения формата медиапространства не мог не сказаться на сути и характере социальных ожиданий людей, часть из которых используют возникший вакуум в противоправных целях, другие продолжают верить «чудесам» и приближению светлого будущего, третьи становятся заложниками нелепого доверия и в конечном итоге потерпевшими.

Как следствие, мы все чаще стали замечать негативные последствия влияния информационных технологий и процессов, которые подробно описаны Ю. Ждановым и В. Овчинским[1]. Навязчивая реклама, постановочные шоу-программы, информационные вбросы и фейки, по сути, заполнили медиапространство низкопробными суррогатами, постепенно вытесняя десятилетиями формируемые ценности, установки и мировоззрение. На смену семье и ее ценностям пришли гражданские браки, браки по расчету и даже попытки создания однополых браков. Любовь из разряда исключительно романтичного чувства привязанности и симпатии к другому человеку постепенно превращается в способ удовлетворения сексуальных потребностей или основу реализации меркантильных целей (желание выйти замуж или жениться на богатой особе или успешном человеке). Отношения лояльности, корпоративной преданности и взаимовыгодности затмили чувства долга, нравственной ответственности и солидарности. Подвержена изменению нравственная и социальная основа таких индикаторов массового сознания, мотивации и принципов демократического государства, как честность и справедливость[2]. Перестали быть престижными профессии врача, учителя или инженера. На смену им пришли блогеры, промоутеры, эскортницы и т.д. Как следствие, для определенной части населения, в особенности молодежи, жизненным приоритетом стали, прежде всего, богатство, власть и престиж.

Транслируемые на всю страну передачи и шоу-программы по центральным каналам телевидения о жизни и поступках некоторых «героев» (чаще всего популярных звезд отечественной

---

[1] *Жданов Ю.Н., Овчинский В.С.* Указ. соч.

[2] *Редя Г.К., Барсукова С.А.* Представления о справедливости в современном российском обществе // Изв. высших учебных заведений. Поволжский регион. Общественные науки. University proceedings Volga region. Politics and law: журнал. 2015. № 2(34). С. 131–135.

эстрады и шоу-бизнеса с их извращенными потребностями, любовными романами и т.д.), а также практически бесконтрольные тиражирование и передача через социальные сети любой информации (включая сцены жестокости, сексуальной распущенности, непомерного богатства, вседозволенности и т.д.) привели к тому, что медиапространство, создаваемое электронными средствами коммуникации, стало выступать некой основой формирования негативных свойств и качеств личности, и не только молодых людей. Иными словами, рассматриваемый фактор, считавшийся ранее лишь одним из условий, способствующим совершению преступлений, становится одной из причин преступного поведения. В связи с этим справедливым можно признать замечание академика П.Л. Капицы, который в свое время отмечал, что средства массовой информации так же опасны, как и «средства массового уничтожения»[1].

В советский период с учетом идеологических соображений и наличия жесткой цензуры любой корреспонденции и средств коммуникации поводов для беспокойства и негативного их влияния практически не было. Как следствие, все медиапространство, контролируемое государством, наряду с определенными «перекосами» определяло подчас истинные постулаты и ценности человека, формировало в нем позитивные взгляды и убеждения, способствовало развитию высокого уровня культуры и правосознания. Оно служило важным средством развития общества[2]. На что же сейчас работает медиапространство, чему оно способствует, что формирует?

В погоне за лайками подростки готовы раздеться, выставить напоказ интимные части своего тела, принять участие в любых аморальных и противоправных действиях, совершить суицидальную попытку и т.п. Этот иллюзорный мир, который создает сегодняшнее медиапространство, может иметь и более серьезные последствия. В условиях режимно-карантинных мероприятий резко активизировались услуги различных интернет-агрегаторов и мо-

---

[1] См.: *Буткевич С.А.* Превенция экстремизма и терроризма и деятельность массмедиа: проблемы синтеза и перспективы коллаборации: ученые зап. Крым. федер. ун-та им. В.И. Вернадского. Юрид. науки. 2017. Т. 2 (68). № 1. С. 115–123.

[2] См.: *Дзялошинский И.М.* Российские медиа: проблемы вражды, агрессии, насилия: учеб. пособие. Саратов: Ай Пи Эр Медиа, 2019.

шенников. Создаваемые ими площадки наполняются новым, порой более циничным содержанием, вовлекая в сферу общения все новых и новых членов, апробируя новые способы обмана и получения доходов. Так, стали появляться некие «экспертные» организации, которые готовы за соответствующую плату удалить из контента нежелательную информацию (онлайн-репутацию) с гарантией по ее невосстановлению.

Проводимый в стране Год науки и технологий должен стать началом переломного момента в решении задач по обеспечению законности и правопорядка в стране, оптимизации законодательства о противодействии преступности и коррупции, созданию надежной защиты информационной безопасности. В связи с этим необходимо разработать дополнительные организационно-правовые механизмы определения и устранения потенциальных угроз, в том числе исходящих из медиапространства. В первую очередь государству следует предусмотреть разработку соответствующих «фильтров» контроля за информационными ресурсами и создателями контента с целью привлечения виновных лиц к установленной законом ответственности в случаях использования такой информации в противоправных целях.

Представляется логичным и последовательным создание института криминологической экспертизы, в котором должны быть задействованы представители независимого экспертного сообщества. Создание такого органа позволит определить характер и степень влияния на граждан нежелательной и вредной информации, стратегию и тактику минимизации указанных угроз, четкие критерии для запрета соответствующего контента, основания экспертных заключений по спорным вопросам, возникающим в правоприменительной практике, и т.п.

И последнее, нужно всегда помнить, что пустоты и не заполненные полезной и социально значимой информацией ниши легко заполняются различным суррогатом и низкопробным материалом, который впоследствии опровергнуть и удалить сложно. Да и сотрудникам правоохранительных органов следует быстрее овладеть соответствующими навыками и инновациями в сфере информационных технологий.

А.Г. Горшенков,
Приволжский филиал
Российского государственного
университета правосудия,
кандидат юридических наук, доцент

Г.Г. Горшенков,
Нижегородский институт
управления РАНХиГС,
кандидат юридических наук, доцент

Г.Н. Горшенков,
Нижегородский государственный
университет имени Н.И. Лобачевского,
доктор юридических наук, профессор

Криминологическая экспертиза и информационная безопасность

Вначале о понятиях той и другой категории.

Информация. Существует множество определений этой категории. Оставляя их за пределами предмета наших рассуждений, обратимся к общему понятию информации, которое дано в Толковом словаре русского языка: «сведения об окружающем мире и происходящих в нем процессах, воспринимаемых человеком…»[1].

Разумеется, воспринимаемых *непосредственно* или *опосредованно*, путем сообщений (передачи) сведений.

Это первое. Второе – мы будем вести речь о *массовой информации*, которая определяется Законом Российской Федерации от 27.12.1991 № 2124-I «О средствах массовой информации» (ст. 2) как «предназначенные для неограниченного круга лиц печатные, аудио-, аудиовизуальные и иные сообщения и материалы». Однако при этом массовую информацию рассматриваем в широком значении, т.е. распространяемую не только предусмотренными означенным законом *средствами массовой информации*, но и любыми другими средствами. Все возможные средства распро-

[1] *Ожегов С.И., Шведова Н.Ю.* Толковый словарь русского языка: 80 000 слов и фразеологических выражений. М.: Азбуковник, 1997. С. 250.

странения информации на неопределенный круг лиц или рассеянную аудиторию именуются в данном *контексте средствами массовой коммуникации*.

Информационная безопасность. Определение данного понятия мы также сужаем рамками предмета нашего внимания. Речь не идет о защите информации от различных угроз, например в процесс производства, хранения, передачи информации; мы имеем в виду обеспечение таких условий, в которых затрудняется, а то и исключается возможность причинения информацией вреда человеку как личности, т.е. морального вреда.

Например, профессор А.А. Стрельцов определяет информационную безопасность именно в широком смысле и определяет ряд понятий данного вида безопасности, т.е. относительно человека, общества, государства[1]. Основываясь на подходах ученого, предложим наше представление о данной категории: информационная безопасность заключается в невозможности причинения имущественного и (или) морального вреда путем уголовно-противоправного деяния, предметом которого является информация или информационное воздействие как способ его совершения.

Имеются в виду воздействия публичного характера, с использованием средств массовой коммуникации, в особенности СМИ (клевета, возбуждение ненависти либо вражды, унижение человеческого достоинства, различные призывы – к насильственному изменению конституционного строя Российской Федерации, к осуществлению террористической деятельности, экстремистской деятельности и т.п.).

Криминологическая экспертиза. Применительно к российской «криминологической действительности» данная категория, в отличие от категории «информационная безопасность», является не столько сущей (формализованной), сколько должной, имеющейся в виду. Хотя одна ее разновидность формализована. Мы имеем в виду антикоррупционную экспертизу, или оценку нормативных правовых актов, их проектов в целях выявления в них

[1] *Стрельцов А.А.* Обеспечение информационной безопасности России. Теоретические и методические основы / под ред. В.А. Садовничего, В.П. Шерстюка. М.: МЦНМО, 2002.

факторов, или «производящих сил» в сфере коррупционной правонарушаемости.

Идеи узаконить отношения в области криминологической экспертизы в России высказываются давно. Например, почти 20 лет ученые С.В. Бородин, В.В. Лунеев писали о десятках тысяч банкротств, которые «носят криминальный характер, но все это делается в рамках действующего законодательства»[1]. 10 лет назад российским криминологическим сообществом под руководством профессора А.И. Долговой был разработан проект федерального закона «О криминологической экспертизе»[2].

Однако, несмотря на все усилия криминологов, диссертационные исследования, взывания к законодателю о необходимости принятия закона о криминологической экспертизе, остается «теория мертва». В то время как в Белоруссии, например, институт криминологической экспертизы функционирует с 2007 г.

Четырнадцатилетний опыт соседнего государства не только показал востребованность экспертно-аналитического потенциала криминологии в традиционной законотворческой сфере, и особенно в инновационном криминологическом правотворчестве, но и открыл перспективы применения криминологической экспертизы в другой сфере – экспертной оценки, например, массово-информационной продукции и в целях установления в ней криминогенных, а то и криминалосодержащих элементов. То есть речь идет о необходимости расширения объекта криминологической экспертизы.

В этом плане представляется заслуживающим внимания определение, которое дают белорусские ученые Н.А. Барановский и Н.Н. Шевчук криминологической экспертизе[3]. Основываясь на их определении, представляем следующую формулировку ее дефиниции: *криминологическая экспертиза есть урегулированная нормами права экспертно-аналитическая деятельность, направленная на криминологическую диагностику и обнаружение деструктивных явлений и процессов в реализации законодательных, право-*

---

[1] *Бородин С.В., Лунеев В.В.* О криминологической экспертизе законов и иных нормативных актов // Гос-во и право. 2002. № 6.

[2] Проект федерального закона «О криминологической экспертизе». URL: http://crimas.ru/?p=1685 (дата обращения: 18.01.2021).

[3] См.: *Барановский Н.А., Шевчук Н.Н.* Криминологическая экспертиза в системе предупреждения преступности // Вестн. Полоцкого гос. ун-та. Сер. 1. 2012. № 13.

применительных и иных мер предупредительного воздействия на преступность с целью последующей криминологической корректировки деятельности по разработке и реализации эффективных решений в области противодействия преступности.

Криминологическая экспертология. Инновационный взгляд на востребованность криминологической экспертизы, в том числе, разумеется, и переосмысление ее объекта, обусловливает потребность в соответствующей разработке нового направления в криминологии – *экспертологии*.

Интернет-энциклопедия определяет экспертологию как *межотраслевую* научную дисциплину, объектом исследования которой является экспертиза[1]. Слово «межотраслевая» в настоящем контексте весьма значимо: оно никак не может быть «выкинуто из песни», т.е. из контекста.

В данном случае, обращаясь к информации, порождающей и объединяющей широкий круг проблематики «внутри» и «вокруг» информационной безопасности, мы с особой остротой всматриваемся, вслушиваемся, наконец, вдумываемся в текст, смысл которого порой, кажется, зависит от одного слова, словосочетания. То есть в нем может быть найдено (ученым, публицистом) наиболее выразительное средство языка, передающее научное суждение, общественно-политическое мнение, иное выражение свободомыслия, а кто-то (правоприменитель, эксперт-лингвист) в нем обнаружит то, что не мог вообразить ученый, публицист, а именно элемент «призыва к осуществлению экстремистской деятельности», «унижение чести, достоинства» и т.п.

Естественно, чрезвычайно важно установить, что именно выражает здесь слово, *причинность* какого действия – правомерного или противоправного. В подобном лингвистическом фокусе сошлись в единстве и противоположностях лингвистические и криминологические знания. Так в научном обороте появился редко употребляемый сегодня термин «*лингвистическая криминология*», означающий комплексную науку о языке как криминогенно-криминальном вербальном явлении. Не столько о самом явлении, сколько о том, что его создает и кем оно создается.

Представляется не совсем логичным: ученые-лингвисты в первую очередь проявляют озабоченность тем обстоятельством, что язык не только может способствовать совершению преступ-

[1] URL: https://ru.wikipedia.org/wiki/Экспертиза (дата обращения: 19.01.2021).

ления, но и может быть использован как орудие преступления. Мы, криминологи, в этом отношении, как ни парадоксально, отстаем. Между тем в данном вербальном явлении просматривается определенная и немаловажная область предмета криминологии, его главная составляющая – *причинность* преступности. И в этом отношении как корректное предостережение нам, криминологам, воспринимается следующее высказывание профессионального писателя, политтехнолога С.Н. Магнитова: «*Отказ признавать негативную часть научного предмета делает науку неполноценной, поскольку она перестает решать предметные проблемы…*»[1].

П.И. Иванов,
главный научный сотрудник отдела
по исследованию проблем
отраслевого управления
научно-исследовательского центра
Академии управления МВД России,
доктор юридических наук, профессор

Цифровая реальность и ее влияние на развитие оперативно-розыскной науки

Невольно возникает вопрос, как может повлиять на дальнейшее развитие оперативно-розыскной науки цифровая реальность. Чтобы ответить на этот вопрос, обратимся к обстоятельствам, его обусловливающим. Заметим, что их много. В числе основных обстоятельств:

достижения современной науки и техники, вызванные новой промышленной революцией и ее технологией[2]. Специалисты в области теории оперативно-розыскной деятельности (далее – ОРД) понимают, что это необратимый процесс. Значит, оперативно-розыскная наука должна реагировать на все негативные изменения цифровой среды;

---

[1] *Магнитов С.Н.* Тринитарное языкознание. Гл. 6. URL: http://www.trinitas.ru/rus/doc/0226/002a/02261190.htm (дата обращения: 17.10.2020).

[2] *Жданов Ю.Н., Овчинский В.С.* Киберполиция XXI века: международный опыт. М.: Междунар. отношения, 2020. С. 9.

прогрессивный процесс, сопровождаемый возникновением и развитием киберпреступности;

разворачивание широкомасштабной работы по поиску форм и методов создания кибербезопасности от существующих вызовов (рисков) и угроз. Усиленно прорабатывается вопрос о принятии Конвенции о борьбе с киберпреступностью под эгидой Организации Объединенных Наций. Отдельно взятая страна не в состоянии эффективно противодействовать, так как названное явление носит глобальный (международный) характер;

наличие цифровой среды. Мы оказались в цифровом мире. Это совершенно иные условия, в которых правоохранительные органы продолжают выполнять возложенные на них функции;

появление ранее неизвестных правоохранительной практике угроз. В юридической литературе их справедливо называют новые. Это мошенничество в сфере телекоммуникаций (способы совершения постоянно модернизируются), отмывание (легализация) «грязных» денег и финансирование организованной преступности и терроризма через криптовалюту, «интернет-вещи», теневой интернет, криминальная онлайн-торговля контрафактными товарами, наркоторговля, торговля оружием. Перечень можно продолжить, но уже перечисленные угрозы свидетельствуют о повышенной опасности для общества и государства. От них во многом исходят негативные последствия. Исследователи, например, заговорили о криптопреступлениях. Отсюда невольно задумываешься, как и каким образом от них избавиться или привести их, по мере возможности, в социально приемлемый уровень. В то же время не следует упрощать реально существующие теоретико-прикладные проблемы, связанные с цифровой средой (киберугрозой);

инновации, обусловленные внедрением цифровых технологий в правоохранительную деятельность. Специалисты утверждают, что их внедрение может упрощать многие рутинные задачи, решаемые сегодня, например, полицией. Мы располагаем таким опытом ряда зарубежных стран[1]. В этом плане и в России ведется активная работа[2];

---

[1] См. подробнее*: Жданов Ю.Н., Овчинский В.С.* Указ. соч.

[2] В части, касающейся оперативно-розыскной науки, см. подробнее: *Иванов П.И., Шитов А.С.* Актуальные проблемы цифровизации оперативно-розыскной деятельности // Технологии информационного общества и развитие теории оперативно-розыскной

наконец, цифровизация преступности. В некотором смысле оперативно-розыскная наука[1] стала как ее следствие. Но нельзя рассматривать это как статику, поскольку данный вид науки находится в непрерывном динамическом состоянии, определяя *основные тренды* и подходы к противодействию киберпреступности. И в ней происходит технологическая трансформация (преобразования). Между тем хотелось бы поставить вопрос, готова ли сегодня оперативно-розыскная наука предложить практике рецепты использования искусственного интеллекта при проведении отдельных оперативно-розыскных мероприятий или же документирования преступных действий проверяемых (подозреваемых). Думается, вряд ли. Приведу сравнение с уголовным судопроизводством, тут смело заявляют о возможностях использования цифровых технологий. Мы не думаем, что оперативно-розыскная наука займет в этом плане *позицию догоняющего* из числа отстающих. Мы уверены в том, что у нее найдется потенциал, чтобы не отставать от впереди идущих. Это самодостаточная наука, имеющая собственную историю. Как известно, теория ОРД отпочковалась от криминалистики еще в 50-х гг. XIX в. Многолетняя практика убедилась в том, что ОРД (разумеется, не без достижений науки) сегодня – действенное средство в борьбе с тяжкими и особо тяжкими преступлениями, носящими межрегиональный, межгосударственный и международный характер.

К сожалению, как представляется, оперативно-розыскная наука[2] сегодня находится в своеобразном замкнутом круге цифровых и иных высоких технологий. Она не может пассивно созерцать все это, когда другие области знаний активно предпринимают меры по научному осмыслению сложившейся кримино-

---

деятельности: сб. науч. тр. (Москва, 15 ноября 2019 г.). М.: ФГКУ «ВНИИ МВД России», 2020; *Их же.* К вопросу о важности приспособления механизма противодействия налоговой преступности к цифровой реальности // Искусственный интеллект (Большие данные) на службе полиции: сб. ст. Междунар. науч.-практ. конф. (Москва, 28 ноября 2019 г.) М.: ФГКОУ ВО «Акад. управления МВД России», 2020.

[1] Далее – ведомственная наука. Ведомственная в смысле принадлежности к системе МВД России.

[2] Взаимосвязь между оперативно-розыскной наукой и оперативно-розыскной деятельностью прямая. Если оперативно-розыскная наука представляет собой систему знаний о закономерностях развития цифровой среды и киберпреступности, то оперативно-розыскная деятельность воплощает эти знания в конкретную практику противодействия преступности указанного вида.

генной ситуации и выработке адекватных ей конструктивных решений проблемы.

По большому счету оперативно-розыскная наука оказалась на новом этапе своего развития, обусловленного указанными обстоятельствами. Но она стремится реализовать прорывную идею, суть которой, на наш взгляд, заключается в оптимизации оперативно-розыскной деятельности, обеспечивая опережение противоправных действий как главного принципа ее организации на всех уровнях управления (федеральном, окружном, межрегиональном, региональном, муниципальном (районном). Ведомственная наука должна выдавать научно обоснованные предложения, рекомендации и алгоритмы, разрабатываемые по запросам практических подразделений на основе обобщения и систематизации положительного опыта оперативных подразделений полиции. Как представляется, чтобы объяснить процессы и явления, протекающие в цифровой среде, важно иметь современный понятийно-категориальный аппарат. Пока что многие термины и понятия, обусловленные данной средой, не нашли теоретического осмысления в рамках предмета оперативно-розыскной науки. Например, такие, как оперативно-розыскное противодействие и его механизм; риск-ориентированный подход как метод оперативно-розыскной науки; «реперные» точки оперативно-розыскного воздействия (объекты) и указывающие на них признаки; оперативно-розыскные риски и угрозы, их источники; оперативно-розыскной мониторинг и его содержание; зоны приоритетного мониторинга; рисковые зоны и их определение по совокупности признаков[1]; «паспорт риска». Исследователи по результатам оперативно-розыскного мониторинга предлагают составлять «паспорт риска», чтобы определить, насколько тот или иной объект нуждается в оперативно-розыскном воздействии (контроле).

Эти термины и понятия, на наш взгляд, также должны быть в структуре предмета науки. С их помощью представляется возможным объяснить как внутренние процессы, происходящие в самой ведомственной науке, так и причины и характер внешнего воздействия. Следует заметить, что ведомственная наука, пополняясь новыми понятиями и терминами, расширяет поле своего

[1] Рисковые зоны – звенья (сегменты) экономики, которые в большей степени подвержены влиянию криминальных структур.

влияния, особенно в части рисков и угроз (посредством преимущественно упреждающих действий). Думается, что традиционный подход несколько запаздывает, не реализовав принцип наступательности и опережения противоправных действий криминально активных лиц.

Оперативно-розыскная наука, продуцирующая систему знаний о закономерностях развития киберпреступности в цифровой среде, придерживается одного принципа – сфера познания не имеет национальных границ. Зарубежный опыт для нее – резерв пополнения знаний, передовых технологий, включая информационные. Оперативно-розыскная наука, как и другие, под свой предмет смело адаптирует (преобразует) существующие технологии, чтобы предложить на их основе новые. В то же время ей не чуждо прогнозирование и стратегическое планирование. Со своей стороны считаем целесообразным разработать стратегию внедрения информационных технологий в оперативно-розыскную деятельность. Тогда оперативно-розыскная наука будет знать, куда двигаться дальше и как.

Возвращаясь к новым угрозам, для убедительности приведем данные ведомственной статистики за 8 месяцев 2020 г. о деятельности органов предварительного следствия в системе МВД России по расследованию уголовных дел о фактах мошенничества с использованием мобильных средств связи[1].

В рассматриваемом периоде наблюдается существенный рост количества преступлений, совершенных с использованием IT-технологий и в сфере компьютерной информации. В целом по Российской Федерации зарегистрировано 318,4 тыс. (+76,7%) киберпреступлений. В каждом четвертом регионе России их количество увеличилось в два и более раза.

Более половины (57,3%) IT-преступлений совершено с использованием сети «Интернет» (182 тыс., +90,2%), свыше трети (42,7%) – посредством мобильной связи (135,8 тыс., +100,5%). В 5 раз возросло число преступлений, совершенных с использованием расчетных (пластиковых) карт (122,5 тыс.). Свыше трех

[1] О направлении алгоритма действий следователя на первоначальном этапе расследования дистанционных хищений: письмо Следственного департамента МВД России от 05.10.2020 № 17/3-34272. Документ официально опубликован не был.

четвертей (75,2%) всех киберпреступлений приходится на кражи (110,5 тыс., +89,5%) и мошенничества[1] (128,9 тыс., +76,1%).

Несмотря на сложную ситуацию, органы предварительного следствия проводят комплекс мероприятий, направленных на своевременное раскрытие и расследование указанных преступлений, в том числе путем направления запросов в международные правоохранительные организации и правоохранительные органы иностранных государств в соответствии с международными договорами Российской Федерации.

Давно доказано, что повышения эффективности борьбы с глобальной киберпреступностью можно добиться лишь путем объединения усилий правоохранительных органов на международном уровне. Отдельно взятое государство не в состоянии решить эту задачу. Одна из ключевых составляющих международного сотрудничества – обмен информацией. По мнению большинства специалистов, в данном направлении следует двигаться, так как сегодня это важнейшее условие обеспечения кибербезопасности. Полагаем, что такие вопросы должны охватываться предметом оперативно-розыскной науки и являться объектом пристального внимания.

Одновременно считаем, что успешное решение методологических проблем этой отрасли немыслимо в отрыве от основных положений Концепции научно-технической политики МВД России до 2030 года (Основные положения)[2], поскольку одним из ее принципов является интеграция ведомственной науки, образования и практики. Среди основных направлений Концепции – выявление, пресечение, раскрытие и расследование преступлений (в том числе оперативно-розыскная и экспертно-криминалистическая деятельность), которые должны быть подвергнуты оперативно-розыскной наукой теоретическому осмыслению путем изучения их с позиции исторического, системного (комплексного) подходов. Следует при этом отметить, что одной из целей Концепции выступает совершенствование информационных и коммуникационных технологий, средств связи, системы защиты информации, кибербезопасности. Указанная цель, на наш взгляд, полностью соотносится с интереса-

---

[1] Статьи 159, 159^3 и 159^6 УК РФ.

[2] *Концепция* научно-технической политики МВД России до 2030 года (Основные положения). М.: ФГКОУ ВО «Акад. управления МВД России», 2019.

ми оперативно-розыскной науки. В данном случае также убеждаемся в том, что цифровая реальность и ее влияние на дальнейшее развитие оперативно-розыскной науки – это не надуманная идея, а объективно обусловленный ход событий.

Данный вопрос стал предметом обсуждения на межведомственной конференции «Технологии информационного общества и развитие теории оперативно-розыскной деятельности», которая состоялась во ВНИИ МВД России 15 ноября 2019 г. Участники конференции единодушно высказались, что это будущее теории ОРД, цифровизация в допустимых пределах (с определенными ограничениями) присуща и теории ОРД, которая не может развиваться изолированно, отвергая достижения других отраслей научного знания. Все новое всегда вначале воспринимается с некоторым опасением, безусловно, есть проблемы на пути освоения процесса цифровизации, но они временные и преодолимые.

Другим не менее важным направлением методологии развития оперативно-розыскной науки, на наш взгляд, может стать требование о необходимости снижения *административного давления на бизнес* со стороны правоохранительных органов[1]. Так, эта проблема обсуждалась на Международной конференции-практикуме «Налоговые преступления: вопросы правоприменения», которая состоялась 30 сентября 2020 г.[2] В частности, рассматривались актуальные вопросы, связанные с квалификацией уклонения от уплаты налогов и сборов с организации, с трансформацией полученной налогоплательщиком необоснованной налоговой выгоды путем уклонения от уплаты налогов, с правовой преюдицией в налоговых преступлениях и с соотношением налоговых преступлений и правонарушений, а также с освобождением от уголовной ответственности. Рассматриваемая отрасль знания не может обходить стороной названную проблему, которая требует дальнейших теоретических исследований, поскольку

---

[1] *Иванов П.И., Шитов А.С.* Уголовная политика в области борьбы с налоговой преступностью и особенности ее реализации подразделениями экономической безопасности и противодействия коррупции органов внутренних дел Российской Федерации // Уголовная политика и культура противодействия преступности: материалы Междунар. науч.-практ. конф. (Краснодар, 11 сентября 2020 г.). Краснодар: Краснодар. ун-т МВД России, 2020.

[2] Организована под эгидой автономной некоммерческой организации «Платформа для работы с обращениями предпринимателей».

одним из поручений по реализации Послания Президента Российской Федерации Федеральному Собранию Российской Федерации от 20.02.2019 № Пр-294 стали вопросы, связанные со снижением административного давления на бизнес.

Подводя итог сказанному, отметим следующее.

Во-первых, оперативно-розыскная наука испытывает сегодня ощутимое воздействие со стороны совокупности обстоятельств, связанных с цифровизацией. Методы и технологии *(информационно-телекоммуникационная сеть),* информационно-поисковые системы, автоматизированные банки данных, электронный документооборот и другие новшества, получившие широкое распространение в деятельности оперативных подразделений полиции, – это ответ (реакция) с их стороны на коренные преобразования системы информационных технологий.

Во-вторых, под цифровизацией в настоящей статье понимается процесс перехода с аналоговой формы передачи информации на цифровую. Применительно к оперативно-розыскной деятельности и оперативно-розыскной науке (отдельной отрасли научных знаний о закономерностях развития цифровой среды и киберпреступности) ключевым является цифровая трансформация традиционных сил, средств, методов, форм ОРД и оперативно-розыскных мероприятий. Указанные сведения в конечном итоге будут представлены в цифровой форме.

В-третьих, что касается цифровых технологий, то их мы рассматриваем как *дискретную систему*, которая базируется на способах кодирования и трансляции информационных данных, позволяющих решать разнообразные оперативно-тактические задачи, стоящие перед оперативными подразделениями полиции, за относительно короткие отрезки времени. Теоретическую модель цифровых технологий должна представить оперативно-розыскная наука на основе глубокой проработки теоретико-прикладной проблемы, связанной с киберпреступностью.

В-четвертых, оперативно-розыскная наука, преследуя такую цель, с помощью присущих ей форм и методов погружается в поиск новых знаний о закономерностях развития цифровой среды и киберпреступности, так как разработка прикладных технологических решений для оперативных подразделений полиции – наукоемкий процесс, требующий глубокого и сложного научного обоснования.

Р.Р. Алиуллов,
начальник кафедры
административного права,
административной деятельности
и управления ОВД Казанского
юридического института
МВД России, доктор
юридических наук

В.А. Иванов,
старший оперуполномоченный
отделения по раскрытию краж
с банковских карт граждан
межрайонного отдела № 5
(по борьбе с мошенничествами)
УУР МВД по Удмуртской Республике

О некоторых факторах, способствующих совершению мошенничеств с использованием информационных технологий в банковской сфере

В современных условиях глубокого реформирования всех сфер жизнедеятельности российского общества востребованной и важной задачей является поиск направлений внедрения современных информационно-телекоммуникационных систем. Не случайно государством данной проблематике уделяется пристальное внимание. В частности, Президент России В.В. Путин в своем Послании Федеральному Собранию от 15.01.2020 в числе приоритетов в решении системных проблем сегодняшней экономики назвал внедрение и использование новых технологий и цифровизацию, подготовку современных кадров и создание научно-технологической базы[1] и указал на необходимость подготовки комплексного плана поддержки отрасли, который должен быть включен в национальный план[2].

[1] Послание Президента РФ Федеральному Собранию от 15.01.2020. URL: http://www.kremlin.ru/

[2] Выступление Президента России В.В. Путина на совещании по вопросам развития информационно-коммуникационных технологий и связи, состоявшемся 10 июня 2020 г. в режиме видеоконференции. URL: http://www.kremlin.ru/

Практика показывает, что прогресс в обществе во многом определяется состоянием и функциональной развитостью, мобильностью банковской системы, выступающей одной из важнейших, неотъемлемых составляющих экономики страны и немало использующей в своей работе информационные технологии. Именно финансово-банковская система, являясь основным звеном экономики страны (как и в любом другом государстве), безусловно, должна быть эффективной, способной обеспечивать финансовые интересы личности, общества и государства. В этих целях в последние годы в финансовой отрасли идет процесс активного перехода банковской деятельности и финансовых структур на расчеты с использованием IT-технологий[1].

В то же время, как подтверждает «анализ состояния банковской системы последних лет, процесс становления рыночных отношений сопровождается ежегодным обострением криминогенной ситуации в данной сфере…»[2]. Преступность как закономерное социально-негативное явление[3] проникла и в среду информационных технологий.

За последние 5 лет в целом количество киберпреступлений возросло более чем в 25 раз (с 11 тыс. до 295 тыс.)[4]. Об этом имеются соответствующие официальные подтверждения: в 2017 г. выявлено 90 587 таких преступлений, в 2018 г. – 174 674 (+92,8%), в 2019 г. – 294 409 (68,5%). В 2020 г. зарегистрировано 510 396 деяний (73,4%), среди которых тяжкие и особо тяжкие составили 267 613 (87,5%)[5].

---

[1] *Хисамова З.И.* Уголовно-правовые меры противодействия преступлениям, совершаемым в финансовой сфере с использованием информационно-телекоммуникационных технологий: дис. ... канд. юрид. наук. Краснодар, 2016. С. 4.

[2] *Саркисян М.С.* Противодействие преступлениям, совершаемым в сфере банковской деятельности: дис. ... канд. юрид. наук. М., 2009. С. 3.

[3] *Криминология*: учеб. для вузов / под общ. ред. д-ра юрид. наук, проф. А.И. Долговой. М.: Норма, 2001; *Долгова А.И.* Избр. тр. / [сост. В.В. Меркурьев, О.А Евланова, А.С. Васнецова, Д.А. Соколов]; Акад. Ген. прокуратуры Рос. Федерации. М., 2017. С. 33.

[4] Выступление Генерального прокурора Российской Федерации на расширенном заседании коллегии, посвященном итогам работы органов прокуратуры за 2019 год и задачам по укреплению законности и правопорядка на 2020 год. URL: https://genproc.gov.ru/.

[5] Краткая характеристика состояния преступности в Российской Федерации в период с 2017 по 2020 г. URL:https://мвд.рф /reports/.

Среди названных деяний самым распространенным является мошенничество, совершаемое путем использования различных процедур в информационно-телекоммуникационной системе. В частности, в 2020 г. зарегистрировано 210 493 мошенничества, квалифицируемых по ст. 159 УК РФ, 25 820 мошенничеств с использованием электронных средств платежа (ст. 159^3 УК РФ), 761 мошенничество в сфере компьютерной информации (ст. 159^6 УК РФ).

В основе своей данные преступления предполагают хищение чужого имущества, коим выступают не только финансовые и овеществленные ресурсы, но и информация, имеющаяся в сети, содержащая особую значимость и уникальность как для физических и юридических лиц, так и для государства в целом. Совершение мошеннических действий с использованием информационно-коммуникационных технологий в Российской Федерации признано одной из угроз национальной безопасности[1].

Безусловно, подобное агрессивное развитие событий в рассматриваемой сфере требует принятия незамедлительных и адекватных мер. По нашему мнению, необходимо создать целостную и единую предупредительную систему на общесоциальном, специально-криминологическом и индивидуальном уровне.

В то же время эффективная система профилактики преступлений в целом и мошенничества в банковской сфере, совершаемого с использованием информационных технологий, в частности в Российской Федерации не сформирована. Несмотря на то что в Доктрине информационной безопасности Российской Федерации[2] однозначно определены стратегические цели и основные направления обеспечения информационной безопасности в экономической сфере, к примеру, в Плане работы правительственной комиссии по профилактике правонарушений на 2021 год, утвержденном 25.12.2020, в контексте требований названной доктрины и в связи с сегодняшним состоянием киберпреступлений данные проблемы не

---

[1] *Молчанова Т.В., Аксенов В.А.* Факторы, обусловливающие мошенничество, совершенное с использованием информационно-телекоммуникационных технологий // Вестн. экон. безопасности. 2020. № 2. С. 94.

[2] Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».

рассматривались. Не было их и в предыдущих планах комиссии (см. протоколы заседаний комиссии).

В органах внутренних дел, являющихся среди правоохранительных структур самыми массовыми и выступающими в качестве ведущей организации по профилактике правонарушений[1], не создан четкий учет рассматриваемых преступлений. Так, в официальных статистических данных настораживает ряд обстоятельств, не позволяющих вразумительно представить логическую последовательность назначения приводимых цифр. Из них невозможно выстроить перспективу действий правоохранителей. С одной стороны, понятно, что в количественном выражении рассматриваемые преступления имеют тенденцию к быстрому росту. С другой – статистически изложенная раскрываемость этих преступлений запутанная (к примеру, в 2018 г. из выявленных 174 674 преступлений указано раскрытыми 43 362 (112,3%), в 2019 г. из 294 409 – 65 238 (50,4%), в 2020 г. из 510 396 – 94 942 (45,5%).

Даже в простом математическом исчислении приводимые цифры, естественно, кроме путаницы, ничего дать не могут. А речь сегодня идет о том, чтобы из фиксируемых динамики и тенденции развития цифр о выявляемых преступлениях, совершаемых с использованием высоких информационных технологий, выстроить эффективную систему профилактических мер, могущих защитить граждан, организации и государство в целом. И здесь полагаем уместным привести слова Президента России В.В. Путина, выступавшего 17 марта 2020 г. на расширенном заседании коллегии Генеральной прокуратуры Российской Федерации, о необходимости осуществления глубокого анализа обозначенных проблем и конкретных проработанных мер, направленных на их решение[2].

Причиняемый обществу и государству преступлениями в сфере банковской деятельности вред исчисляется сотнями мил-

---

[1] Постановление Правительства РФ от 28.03.2008 № 216 «О Правительственной комиссии по профилактике правонарушений». Состав комиссии утвержден распоряжением Правительства РФ. Данным нормативным актом Председателем комиссии назначен Министр внутренних дел Российской Федерации.

[2] Выступление Президента России В.В. Путина на расширенном заседании коллегии Генеральной прокуратуры Российской Федерации, посвященном итогам работы органов прокуратуры за 2019 год и задачам по укреплению законности и правопорядка на 2020 год. URL: https://genproc.gov.ru/.

лиардов долларов[1]. И, безусловно, подобное развитие событий становится проблемным в целом для российского общества, особенно в условиях сохраняющихся угроз экономической и национальной безопасности[2].

И здесь нельзя не согласиться с А.Ю. Олимпиевым и А.Ю. Александровой о распространенности в кредитно-банковской системе преступлений, совершаемых путем мошенничества[3]. Полагаем, что и призыв Президента России В.В. Путина в Послании Федеральному Собранию от 15.01.2020 о настоятельной потребности «…ускорить рассмотрение технологического законодательного пакета», запуске уже в текущем году гибкого механизма экспериментальных правовых режимов для разработки и внедрения в России новых технологий, наладить современное регулирование оборота больших данных[4] следует признать своевременным и обнадеживающим.

По нашему мнению, до настоящего времени Федеральный закон от 23.06.2016 № 182-ФЗ «Об основах системы профилактики правонарушений в Российской Федерации» не совсем полно и системно регламентирует как общие вопросы предупреждения правонарушений, так и вопросы профилактики ее экономической составляющей. В частности, ст.15 названного закона определяет двухуровневую систему профилактики правонарушений: общую и индивидуальную. Полагаем, что в науке, законодательстве и практике правоприменения устоялась и реализуется трехзвенная система профилактики преступлений, позволяющая эффективно противостоять преступности в целом и экономической ее составляющей в частности.

---

[1] *Чекунов И.Г.* Киберпреступность: понятие и классификация // Рос. следователь. 2012. № 2; *Урбан В.В.* Преступления, совершаемые с использованием информационно-телекоммуникационных сетей: общая характеристика и уголовно-процессуальные меры по их противодействию // Вестн. Восточно-Сибир. ин-та МВД России. 2019. № 1 (88). С. 57.

[2] Указы Президента РФ от 31.12.2015 № 683 «О Стратегии национальной безопасности Российской Федерации» и от 13.05.2017 № 208 «О Стратегии экономической безопасности Российской Федерации на период до 2030 года».

[3] *Олимпиев А.Ю., Александрова А.Ю.* Общая характеристика преступлений в сфере кредитно-банковской деятельности по УК РФ 1996 г. (понятие, система, виды преступлений, причины) // Вестн. экон. безопасности. 2019. № 2. С.146.

[4] Послание Президента РФ Федеральному Собранию РФ от 15.01.2020. URL: http://www.kremlin.ru/

В связи с этим предлагаем следующую редакцию ст. 15 Федерального закона «Об основах системы профилактики правонарушений в Российской Федерации»:

«Статья 15. Виды профилактики правонарушений

1. Профилактика правонарушений осуществляется на общесоциальном, специально-криминологическом, индивидуальном уровнях и направлена на их минимизацию.

2. Общесоциальная профилактика правонарушений направлена на обеспечение эффективности экономической, политической, идеологической сфер функционирования государства, охватывает наиболее крупные и имеющие стратегический, долговременный характер.

3. Специально-криминологическая профилактика направлена на выявление и устранение причин правонарушений и условий, способствующих совершению правонарушений или облегчающих их совершение, а также на повышение уровня правовой грамотности и развитие правосознания граждан.

4. Индивидуальная профилактика правонарушений осуществляется в целях воспитания и перевоспитания граждан, а также оказания помощи лицам, пострадавшим от правонарушений или подверженным риску стать таковыми.».

Полагаем, что данная редакция предлагаемой нормы полно регламентирует систему профилактики правонарушений в стране и позволит обеспечить эффективность противодействия в сфере экономики в целом и совершению мошенничеств с использованием информационных технологий в банковской сфере в частности.

Ю.А. Воронин,
профессор кафедры уголовного
и уголовно-исполнительного
права, криминологии
Южно-Уральского
государственного университета,
доктор юридических наук

Основные тенденции преступности в цифровой сфере

1. Устоявшейся в российской криминологии является трактовка цифровой преступности (или информационно-цифровой преступности) как понятия и соответствующего явления, представляющего собой широкий круг общественно опасных деяний, совершенных в информационно-коммуникационной среде с использованием цифровой информации и информационно-коммуникационных технологий. В связи с этим есть основание констатировать, что одной из актуальных задач криминологической науки и практики является комплексный анализ состояния и тенденций цифровой преступности, изучение обстоятельств, ее детерминирующих или стимулирующих[1].

Существующее разнообразие преступных проявлений, связанных с информационно-цифровой средой (по предмету общественно опасных посягательств или способам их совершения), делает чрезвычайно сложным исчерпывающий обзор их состояния и эволюции. Несмотря на это, с учетом степени распространенности и динамики проявлений таких общественно опасных деяний попытки решения задачи их классификации и выделения тенденций их развития неоднократно предпринимались различными исследователями. Особенно плодотворным явился подход к проблеме, предложенный российским криминологом В.С. Овчинским[2].

---

[1] *Воронин Ю.А.* Преступления в сфере обращения цифровой информации и их детерминанты // Виктимология. 2020. № 1 (23). С. 76.

[2] *Овчинский В.С.* Цифровое общество: преступление и наказание: интервью в интернет-портале «Лица». 30.01.2018. URL: http//2035.media/2018/01/30ovchinskiy-interviiew/ (дата обращения: 02.01.2020).

Говоря о существовании наиболее заметных современных тенденций в информационно-цифровой преступности, есть основания диагностировать наличие ряда приобретающих все более заметное развитие в криминальной среде специфических характеристик по сравнению с типичными, устоявшимися на протяжении многих десятилетий чертами.

2. Так, анализ сложившейся криминогенной ситуации свидетельствует, что среди наиболее существенных факторов, оказывающих прямое воздействие на изменение характеристик преступных проявлений, прежде всего следует назвать получение преступниками в результате информационно-цифрового бума возможности обладать чрезвычайно эффективными, не существовавшими ранее технологиями, открывающими новые перспективы для совершения преступлений. *В первую очередь информационно-цифровые средства расширили возможности организованных преступных сообществ. Речь идет о развитии генеральной тенденции, а именно: о влиянии информационно-цифровой среды прежде всего на рост организованной преступности, активно использующей цифровые технологии, электронно-вычислительную технику. Особенно это относится к небывалому развитию высокотехнологичной (так называемой цифровой) транснациональной (территориально) и многонациональной (по своему составу) организованной преступности.*

Указанная тенденция выразилась, во-первых, в ускорении динамики вовлечения в ряды транснациональных преступных сообществ этнических представителей самых разных стран, т.е. в своеобразную «интернационализацию» состава этих преступных группировок. Достаточно сказать, что в транснациональной криминальной активности организованных преступных формирований с различным этническим составом сегодня принимают участие выходцы примерно из 80% стран мирового сообщества. Во-вторых, развитие анализируемой тенденции нашло отражение в усилении диверсификации криминальной активности организованных преступных сообществ именно на международном, транснациональном уровне, т.е. на территории ряда государств. Высокотехнологичные транснациональные преступные группы стремительно расширяют свою специализацию и демонстрируют все более высокие «показатели экономической эффективности».

3. Еще одной из стремительно набирающих обороты тенденций развития цифровой преступности является *активизация криминалитета в связи с операциями с использованием виртуальных денег, в том числе биткоина*. Подоплека сложившейся ситуации ясна. Во-первых, мафиозные структуры, широко используя квалифицированных программистов, специалистов по видеонаблюдению, манипуляторов с виртуальной валютой, «зарабатывают» на этом огромные суммы[1]. Во-вторых, именно в силу «продвинутости» этой (в отличие от традиционных) сферы и способа мошеннических действий преступников подобная активность является такой эффективной. Наконец, в-третьих, она опять-таки чрезвычайно привлекательна из-за высокого уровня конспиративности и, следовательно, безнаказанности этого преступного бизнеса. Ведь в подобных случаях, несмотря на предпринимаемые усилия, спецслужбы обладают сравнительно ограниченными возможностями для отслеживания денежных потоков нелегального характера, выявления и наказания виновных в криминальных операциях лиц.

4. Но наиболее динамичной, стремительно развивающейся в плане технической изощренности (несмотря на кажущуюся традиционность) является *тенденция, характеризующаяся самым широким спектром преступных деяний именно с корыстной мотивацией и с использованием компьютерной техники, т.е., по сути, цифровых технологий*. Речь идет о мошенничестве, связанном с применением компьютеров; подлоге, сопровождающемся использованием компьютерной техники; фишинге; краже персональных данных в корыстных целях.

В частности, как справедливо подчеркивается специалистами, одним из самых распространенных преступлений среди этого перечня прежде всего является *компьютерное мошенничество в сети «Интернет»*. Современная тенденция стремительного роста именно данной цифровой преступности не случайна. Интернет-технологии позволяют преступникам применять для сокрытия своих персональных данных программные инструменты. К наиболее популярным разновидностям мошеннических преступлений дан-

---

[1] *Воронин Ю.А.* Криминогенные факторы в информационно-цифровой среде // Smart Law for Smart Industry: сб. науч. ст. М.: Проспект, 2020. С. 178–179.

ной категории в настоящее время относятся компьютерные мошенничества с онлайновыми аукционами, получившими распространенность в ряду услуг электронной торговли. Мошенники на аукционных площадках используют отсутствие личного контакта между продавцом и покупателем. В результате трудности, связанные с нахождением различия между настоящим пользователем и преступником, приводят к тому, что мошенничество с аукционами стало одним из самых популярных видов преступлений. Что же касается самых распространенных методов осуществления таких преступных деяний, то к ним относятся выставление на продажу несуществующих товаров и требований авансовой оплаты покупки до ее доставки, а также покупка товаров и просьба их доставить, но без намерения оплатить эти товары[1].

Далее. *Подлог, связанный с применением компьютеров и зачастую основного составляющего элемента такого подлога – фишинга,* – это также разновидность наиболее активно распространяющихся цифровых преступлений. Свидетельство тому – продолжающееся увеличение объема и эффективность фишинговых компаний. Если раньше в основном их адресатами были отдельные граждане, то теперь фишинговые атаки стали в больших масштабах осуществляться против частного и корпоративного секторов, особенно банков и других расчетных систем. Подоплека такой широкой экспансии проста. Дело прежде всего в относительной простоте и результативности фишинговой технологии. Правонарушители разработали и используют методы, предотвращающие осознание конкретным пользователем того факта, что он введен в заблуждение. Злоумышленники приобретают набор уязвимых сайтов различной тематики. Обладая даже ограниченным доступом к таким сайтам, они могут изменять их таким образом, чтобы часть их посетителей перенаправлялась на фишинговую страницу. Если пользователь зашел на «поломанный» сайт в результате поискового запроса в системах Google, Yandex, Bing, Rambler, Mail.ru, то его перенаправляют на фишинговый сайт. При этом переход жертвы может быть осуществлен на любую страницу «поломанного» сайта, кроме главной, иначе

[1] *Овчинский В.С.* Криминология цифрового мира: учеб. для магистратуры. М.: Норма; ИНФРА-М, 2018. С. 10–11, 68–113.

перенаправление на фишинговый сайт не осуществляется. Фишинговый сайт замаскирован, как правило, под акцию по розыгрышу призов и информирует потерпевшего о выигрыше денежного приза и возможности получить деньги. Но для этого злоумышленники просят указать реквизиты банковской карты. Как только личная информация владельца сайта раскрыта, правонарушители входят в учетные записи жертв и осуществляют перевод денежных средств на новые счета.

Сродни фишингу выступает набирающее в России интенсивные обороты *телефонное мошенничество с помощью роботов*, при котором первоначальный обзвон потерпевших проводят автоматизированные центры. Злоумышленники могут звонить с поддельных номеров, используя сервисы IP-телефонии, WhatsApp, Viber и т.д. О стремительности роста этой разновидности криминальных манипуляций свидетельствуют данные ведомственной банковской статистики. Так, только в течение 2020 г. службами безопасности Сбербанка России зарегистрировано более трех миллионов попыток телефонного мошенничества в отношении его клиентов, что вдвое больше, чем в 2019 г.

К сказанному уместно добавить, что помимо упомянутых *многие из существовавших тенденций корыстной цифровой преступности не остаются стабильно неизменными.* Это, в частности, относится к кибервымогательству, мелким хищениям с помощью вредоносного софта, использованию банковских троянов. Против ожиданий перечисленные виды относительно незамысловатой корыстной цифровой киберпреступности не растворились в высокотехнологичном цифровом криминале, а продолжают стабильно нарастать по объемам.

В целом же, по оценкам экспертов, мировой ущерб от всех рассмотренных разновидностей цифровых преступлений с корыстной мотивацией в годовом исчислении составляет примерно 600 млрд долл. – при росте на десятки процентов ежегодно[1]. Представляется, что эта ситуация будет сохраняться долго, будучи очевидно востребованной криминальным рынком.

---

[1] *Сюнтюренко О.В.* Цифровая среда: тренды и риски развития // Науч.-техн. информ. Сер. 1. Организация и методика информационной работы. М.: ВИНИТИ РАН, 2015. № 2.

5. Наконец, было бы ошибкой игнорировать особенно опасную специфическую составляющую среди тенденций цифровой преступности, а именно: *заметным трендом двух минувших десятилетий стало частое осуществление экстремистских и террористических преступлений с использованием компьютерных инструментов, масштабных и изощренных DDoS-атак в комбинации с сетевыми атаками по выведению из строя систем информационной безопасности.*

Прежде всего следует упомянуть об использовании террористами сети «Интернет», облачных технологий для кибератак на важнейшие оборонные объекты, объекты энергетической, промышленной инфраструктуры и другие важнейшие системы жизнеобеспечения населения, вредоносных программ для цифровых диверсий. Важнейшей составляющей анализируемой тенденции является также проникновение террористов на веб-сайты финансовых структур, получение информации о кредитных картах частных лиц с последующим изъятием денежных средств.

Существенным элементом тенденции криминального использования террористами и экстремистами цифровой сферы является идеологическая обработка и вербовка контингента лиц для совершения насильственных действий на основе экстремистских идеологий или в террористических целях. Этот процесс включает использование пропаганды, которая на протяжении длительного времени ведется посредством сети «Интернет». Обычно такие пропагандистские материалы имеют форму мультимедийных коммуникаций и содержат идеологические или практические разъяснения, рекомендации или рекламу террористической, экстремистской деятельности. Сюда относятся виртуальные сообщения, презентации, журналы, теоретические работы, аудио- и видеофайлы, разрабатываемые террористическими, экстремистскими организациями.

Специалисты отмечают, что широкая область влияния распространяемой через сеть информации в геометрической прогрессии увеличивает аудиторию, на которую она может воздействовать. Интернет-пропаганда также может включать такой контент, как видеосюжеты о насильственных, террористических актах или создаваемые террористическими организациями видеоигры, имитирующие акты терроризма и побуждающие пользова-

телей участвовать в игре, выступая в роли виртуального террориста[1]. Таким образом, оборотной стороной технологического прогресса явилось получение террористами, а также экстремистски настроенными лицами и организациями арсенала цифровых средств и методов для использования их в противоправных целях.

6. В заключение краткого анализа современных тенденций цифровой преступности следует подчеркнуть, что неуклонно прогрессирующий уровень кибермошенничества, компьютерного шантажа и террористических угроз требует разработки и практического осуществления мер, направленных на эффективное противодействие дальнейшему развитию этих тенденций как в общеуголовной, так и в террористической цифровой преступности, а значит, диктует необходимость усиления государственного контроля за состоянием информационно-цифровой среды.

Н.А. Швед,
заместитель начальника отдела
ГУ «Научно-практический центр
проблем укрепления законности
и правопорядка Генеральной
прокуратуры Республики Беларусь»,
кандидат юридических наук, доцент

Цифровые технологии и уголовное право

Развитие цифровых технологий затрагивает не только территорию отдельно взятых государств, но и общемировое экономическое пространство в целом, формируя при этом новые вызовы обществу. Следствием глобальной цифровизации явилось изменение облика преступности в целом, которая в связи с использованием указанных технологий приобрела не свойственные ей ранее признаки.

[1] *Овчинский В.С.* Цифровое общество: преступление и наказание: интервью в интернет-портале «Лица». С. 71–72.

Конечно, в связи с проникновением информационных цифровых технологий в разные сферы жизнедеятельности общества в последние годы совершенствуются уголовно-правовые механизмы обеспечения безопасности в информационно-коммуникативном пространстве: устанавливается уголовная ответственность за совершение ранее криминализированных деяний с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет». Как правило, законодатель идет в данных случаях по пути конструирования квалифицированных составов. Однако этого недостаточно, ведь новые реалии требуют нового правового регулирования, способного адекватно и оперативно отвечать вызовам современности. И, к сожалению, не всегда действующее уголовное законодательство может быть применимо в новых условиях.

Нами уже отмечалась необходимость формирования нового правового регулирования, в том числе и при помощи уголовно-правовых норм[1].

Р.Н. Ключко также отмечает, что в целях защиты интересов субъектов информационных отношений необходимо обеспечить криминализацию общественно опасных информационных деяний, которая должна быть своевременной, с обеспечением системности уголовного законодательства и согласованности уголовно-правовых норм с нормами регулятивных отраслей права[2]. При этом, как совершенно справедливо отмечает Н.В. Воронов, возникает определенная двойственность, где, с одной стороны, уголовное право призвано регулировать общественные отношения, в том числе в сфере цифрового пространства, с другой – право должно способствовать цифровому прогрессу и формированию цифрового сообщества, не создавая при этом излишних препятствий[3].

---

[1] *Швед Н.А.* Уголовная политика Республики Беларусь в сфере информационной безопасности // Право в соврем. белорусском обществе: сб. науч. тр. Нац. центр законодательства и правовых исслед. Респ. Беларусь; редкол. Н.А. Карпович (гл. ред.) [и др.]. Минск: Бизнесофсет, 2017. Вып.12. С. 793.

[2] *Ключко Р.Н.* Уголовно-правовая охрана информационных отношений: перспективы совершенствования // Противодействие киберпреступности: соврем. состояние и пути повышения эффективности: сб. ст. / Следств. ком. Респ. Беларусь; редкол. С.Я. Аземша (гл. ред.) [и др.]. Минск: ЮрСпектр, 2020. С. 151.

[3] *Воронов В.Н.* Уголовно-правовые риски развития цифровых технологий: постановка проблемы и методы научного исследования // Вестн. Ун-та им. О.Е. Кутафина (МГЮА). 2018. № 12. С. 76.

В связи с этим хотелось бы обозначить ряд проблемных вопросов, которые в условиях поступательной цифровой трансформации общества и экономики неизбежно придется решать в ближайшее время.

Особую актуальность приобретает обеспечение информационной безопасности. При этом можно выделить несколько направлений. Сегодня использование компьютерных средств и телекоммуникаций является необходимой и неотъемлемой частью жизни практически каждого человека и современного общества. На базе ИКТ создается комплексная инфраструктура для оказания населению множества электронных услуг, формируются различного рода базы данных, накапливаются массивы информации, что ставит вопрос об обеспечении информационной безопасности личности, защите персональных данных, обеспечении безопасного пользования указанной инфраструктурой. В случае нарушения прав и свобод человека в информационной сфере государство в необходимых случаях может и должно использовать уголовно-правовые меры борьбы с посягательствами такого рода.

Весьма актуален вопрос о защите детей от дестабилизирующего воздействия информационной продукции путем сохранения их психического, психологического здоровья и благополучия, а также формирования позитивного мировосприятия. Увеличение числа несовершеннолетних пользователей сети «Интернет» обусловливает необходимость совершенствования уголовного законодательства в целях обеспечения не только информационной безопасности детей, но и зачастую безопасности их жизни и здоровья.

Важное место в структуре информационной безопасности принадлежит обеспечению информационной безопасности экономической деятельности, поскольку эффективная экономическая активность граждан и организаций переходит в формат цифровой экономики. Киберугрозы, связанные с хищением цифровых денежных активов, хакерские атаки, инсайдерская торговля, преступные посягательства в инновационной сфере и другие проявления становятся глобальной проблемой современности. Не случайно цифровая трансформация бизнес-процессов и технологий увеличивает расходы на информационную безопасность и инфраструктуру.

Последствия процесса цифровизации финансов, распространения новых технологий и инструментов, начавшегося в связи с четвертой промышленной революцией, точно сейчас спрогнозировать невозможно. Несомненно, что денежно-кредитная система по мере цифровизации становится все более уязвимой. Кризисные явления, возникая в отдельных организациях и (или) сегментах финансового рынка, с легкостью переносятся на всю систему[1].

Действительно, активное развитие банковских электронных услуг и более широкое предоставление клиентам банков удаленного доступа к их счетам для совершения платежей и переводов также влечет возникновение угроз криминального характера. Речь может идти и о высокотехнологичных формах хакерских атак, и о различного рода мошеннических действиях, в результате чего владелец счета либо сам переводит свои средства на счет преступников, либо раскрывает всю конфиденциальную информацию (например, свои персональные данные, данные платежных карт, пароли, коды и т.п.), необходимую для получения доступа к счету. Кроме того, общественную опасность указанных деяний усиливает специфика способа совершения преступления – использование удаленного доступа к банковскому счету при помощи технических средств, что позволяет лицу оставаться анонимным и совершать преступление из любой точки мира, имея лишь доступ к сети «Интернет».

В качестве примера использования новых цифровых реалий для совершения преступлений можно привести и криптовалюты, которые становятся все более популярными не только среди представителей бизнеса, граждан, но и в криминальной среде. Так, среди основных рисков оборота криптовалют выделяют финансирование терроризма, совершение киберпреступлений и легализацию доходов, добытых преступным путем. Криптовалюта может выступать предметом хищений, преступлений коррупционного характера, экономических и других общеуголовных преступлений. В числе криминогенных свойств криптовалют отмечают анонимность переводов, скорость транзакций, запутанные цепочки транзакций и др.

---

[1] *Тихонов О., Лобанов А.* Угрозы и вызовы XXI: стратегия реагирования // Банкаўскі весн. 2020. № 1. С. 16.

Криптовалюта используется в том числе на площадках Darknet как инструмент торговли изъятыми из оборота товарами: похищенными реквизитами банковских карт, поддельными деньгами, детской порнографией, персональными данными, психоактивными веществами и др.[1] М.М. Долгиева справедливо отмечает, что криптовалютные отношения, несмотря на их полное присутствие во многих областях деятельности человека и государства, еще не признаны объектом уголовно-правовой охраны в теоретическом плане и на законодательном уровне[2].

Еще одним продуктом цифровизации, представляющим интерес для сферы уголовно-правового регулирования, является искусственный интеллект. Так, ученые отмечают необходимость правового обеспечения использования техники с элементами искусственного интеллекта в различных сферах человеческой деятельности. В качестве примера А.Л. Савенок приводит использование беспилотной техники, в частности беспилотных автомобилей, медицинских и промышленных роботов[3].

Л.В. Павлова полагает целесообразным усиление требований к деятельности, связанной с использованием искусственного интеллекта и представляющей риск для жизни человека, в частности государственной регистрации вводимых в эксплуатацию отдельных видов искусственного интеллекта, их производителей и владельцев, использование режима видеорегистрации не только осуществляемых искусственным интеллектом операций, но и окружающей обстановки и др.[4]

---

[1] *Харчейкина Ю.В.* Криминальное использование криптовалюты: проблемы противодействия // Совершенствование следственной деятельности в условиях информатизации: сб. материалов междунар. науч.-практ. конф. Минск, 12–13 апр. 2018 г. / Следств. ком. Респ. Беларусь; редкол. С.Я. Аземша [и др.]. Минск, 2018. С. 343.

[2] *Долгиева М.М.* Квалификация преступлений, совершаемых в сфере компьютерной информации в отношении криптовалюты // Соврем. право. 2018. № 11. С. 103.

[3] *Савенок А.Л.* Человек. Право. Техника // Человек и право: проблема ценностных оснований правового регулирования: материалы V Междунар. науч. конф. по проблемам клас. и постклас. методологии юрид. науки. Минск, 3–4 мая 2019 г. / под ред. В.И. Павлова, А.Л. Савенка. Минск, 2019. С. 194.

[4] *Павлова Л.В.* Техноэтика и вопросы искусственного интеллекта с точки зрения уголовно-правовой науки // Противодействие киберпреступности: соврем. состояние и пути повышения эффективности: сб. ст. / Следств. ком. Респ. Беларусь; редкол.: С.Я. Аземша (гл. ред.) [и др.]. С. 217.

Решение указанных и ряда иных вопросов, обусловленных развитием цифровых технологий, возможно после разработки регулятивного механизма использования искусственного интеллекта, больших данных, цифровых активов, определения правового статуса субъектов интернет-пространства и др. При этом следует отметить, что развитие цифровых технологий требует от субъектов правотворчества и сопоставления уровня цифровизации общественных отношений и уголовного закона, оценки принципов действия уголовного закона по кругу лиц, в пространстве и во времени, вины, соучастия и иных институтов уголовного права на возможность их применения в новых реалиях, и, при необходимости, корреляции их с учетом новых вызовов и угроз. Кроме того, как отмечают в научной литературе, можно спрогнозировать и самую глобальную проблему: трансформации классических подходов к пониманию парадигмы преступления как явления реальной, объективной действительности с учетом появления действительности виртуальной и возможных угроз ее использования для причинения вреда уже существующим и в перспективе способным появиться объектам уголовно-правовой охраны[1].

Таким образом, приведение в соответствие положений уголовного права с последствиями глобальной информатизации и цифровизации общественных отношений видится перспективной задачей, которую следует решать в самое ближайшее время. Сформировавшиеся в последние годы новые формы преступной деятельности с использованием самых современных ИКТ нельзя оставлять без внимания. Представляется, что именно уголовно-правовой запрет как наиболее эффективная мера защиты должен играть важную превентивную роль в условиях динамичного развития информатизации общества и цифровой трансформации экономики.

[1] *Ключко Р.Н.* Указ. соч. С. 151.

Л.В. Иванова,
доцент кафедры уголовного
права и процесса Тюменского
государственного университета,
кандидат юридических наук,
доцент

Уголовно-правовое противодействие киберпреступности в странах БРИКС

В Московской декларации XII саммита БРИКС, состоявшегося 17 ноября 2020 г.[1], признается проблема все возрастающего использования информационно-коммуникационных технологий в преступных целях и отмечается важность разработки единой нормативно-правовой базы для противодействия этому.

Несмотря на общность интересов в противодействии киберпреступности, подходы к криминализации нарушений в цифровом пространстве в рамках конкретного государства существенно различаются как по форме, так и по содержанию. Рассмотрим особенности закрепления уголовной ответственности за киберпреступления в законодательстве стран, входящих в БРИКС (Федеративная Республика Бразилия, Российская Федерация, Республика Индия, Китайская Народная Республика и Южно-Африканская Республика).

Единственным источником уголовной ответственности в Российской Федерации является УК РФ, из содержания которого можно сделать вывод о наличии двух групп киберпреступлений: специальные киберпреступления (преступления в сфере компьютерной информации) и общеуголовные киберпреступления (все иные, совершаемые с использованием информационных технологий)[2].

В Уголовном кодексе Бразилии[3] статьи о киберпреступлениях содержатся в разных главах. При этом в последние годы законодатель стремится установить наказание за новые виды пре-

[1] URL: https://brics-russia2020.ru/images/114/83/1148395.pdf (дата обращения: 25.01.2021).
[2] См. подробнее: *Иванова Л.В.* Виды киберпреступлений по российскому уголовному законодательству // Юрид. исслед. 2019. № 1.
[3] Código Penal (Decreto-Lei № 2.848, de 7 de Dezembro de 1940). URL: http://www.planalto.gov.br/CCIVIL_03/Decreto-Lei/Del2848.htm#art334 (дата обращения: 20.01.2021).

ступлений, совершаемых с использованием информационных технологий.

Так, 26 декабря 2019 г. в ст. 122 УК Бразилии были внесены изменения[1], предусматривающие усиление ответственности в случае побуждения, подстрекательства, содействия самоубийству или членовредительству, осуществленного через компьютерную сеть, социальную сеть или передачу в реальном времени.

С 2018 г. установлена уголовная ответственность за распространение материалов порнографического содержания через средства массовой информации, компьютерную или телекоммуникационную систему.

С 2013 г. УК Бразилии устанавливает ответственность за прерывание или нарушение работы телематических или информационных служб общественного пользования. Ранее закон защищал только телеграфные или телефонные связи.

При этом любое преступление, совершенное в киберпространстве, может быть наказано так же, как если бы оно было совершено вне такого контекста. Кроме того, иногда в статьях конкретно не упоминаются информационные и телекоммуникационные сети как способ совершения преступления, но это может подразумеваться в тексте закона, поскольку в статье упоминается публичное совершение преступления.

Помимо Уголовного кодекса в Бразилии действуют и специальные законы, в которых может устанавливаться ответственность за соответствующее преступление в киберпространстве. Например, Закон о промышленной собственности[2] закрепляет ответственность за публикацию любым способом ложной информации в ущерб конкуренту с целью получения преимущества. Использование любых средств публикации включает использование и информационных технологий.

В Индии можно выделить три группы киберпреступлений. Первая группа преступлений выделяется в соответствии с Законом об информационных технологиях[3], вторая группа – в соот-

---

[1] Lei n 13.718, de 24 de setembro de 2018. URL: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13718.htm (дата обращения: 20.01.2021).

[2] Industrial Property Law. 9,779/96. URL: https://www.jpo.go.jp/e/system/laws/gaikoku/document/index/brazil-e_industrial_property_law.pdf (дата обращения: 20.01.2021).

[3] The Information Technology Act, 2000. URL: https://www.indiacode.nic.in/bitstream/123456789/1999/3/A2000-21.pdf (дата обращения: 20.01.2021).

ветствии с Уголовным кодексом Индии[1], а третья группа преступлений – в соответствии со специальными и местными законами.

Закон об информационных технологиях является основным законодательным актом Индии, касающимся киберпреступлений, в гл. XI которого содержится обширный и подробный перечень киберпреступлений и наказаний за них (ст. 65–74). Единственным преступлением, за которое может грозить пожизненное лишение свободы, является кибертерроризм.

Уголовный кодекс Индии содержит несколько киберпреступлений, например киберпреследование, сексуальные домогательства в электронном виде, фейковые новости в социальных сетях.

Иногда формулирование способа совершения преступления указывает на возможность совершения преступления посредством информационно-телекоммуникационных сетей. Среди таких преступлений можно назвать подстрекательство к мятежу, клевету и др.

Если в законе информационные технологии не указываются в составе конкретного преступления, но фактически преступление было совершено в сети «Интернет», то в статистике такое преступление отражается как киберпреступление. Например, подстрекательство к самоубийству может происходить в сети, и в этом случае оно становится киберпреступлением.

Последняя группа киберпреступлений – это преступления, предусмотренные специальными законами: Законом об азартных играх[2], Законом о лотереях[3] и др. Уголовная ответственность одновременно возможна в соответствии как с Уголовным кодексом Индии, так и со специальным законом.

В Уголовном кодексе Китайской Народной Республики[4] установлена ответственность за такие киберпреступления, как незакон-

---

[1] The Indian Penal Code, 1860. URL: https://www.indiacode.nic.in/handle/123456789/2263?locale=en (дата обращения: 20.01.2021).

[2] The Public Gambling Act, 1867. Digital Repository of All Central and State Acts. URL: https://www.indiacode.nic.in/handle/123456789/2269?view_type=browse&sam_handle=123456789/1362 (дата обращения: 20.01.2021).

[3] The Lotteries (Regulation) Act, 1998. Digital Repository of All Central and State Acts. URL: https://www.indiacode.nic.in/handle/123456789/1994?view_type=browse&sam_handle=123456789/1362 (дата обращения: 20.01.2021).

[4] Criminal Law of the People's Republic of China. URL: http://www.chnlawyer.net/law/subs/xingfa.html (дата обращения: 20.01.2021).

ное вторжение в компьютерную информационную систему, уничтожение компьютерных информационных систем, невыполнение обязательств по управлению безопасностью информационной сети, незаконное использование информационных сетей. В ряде статей использование информационных технологий не упоминается, но подразумевается в способе совершения преступления.

Поскольку киберпреступления разнообразны, трудно предвидеть, какие конкретные деяния будут совершены с помощью телекоммуникационных сетей. Для этих целей представляется важной ст. 287 УК Китая, согласно которой «кто использует компьютеры для совершения финансового мошенничества, кражи, растраты, растраты государственных средств, кражи государственной тайны или других преступлений, должен быть осужден и наказан согласно соответствующим положениям этого кодекса».

В Южно-Африканской Республике положения об уголовной ответственности за киберпреступления содержатся в различных нормативных актах, охраняющих определенную область цифровой среды. Действующее право представляет собой гибрид различных законодательных актов и общего права.

Например, действует Закон о защите критической инфраструктуры[1], в котором предусмотрена ответственность за предоставление, распространение или публикацию любым способом информации, относящейся к мерам безопасности, применяемым в критической инфраструктуре или в отношении нее.

Однако термин «киберпреступления» называется в Законе об электронных коммуникациях и сделках[2], гл. VIII которого включает такие преступления, как несанкционированный доступ, перехват или вмешательство в данные, а также компьютерное вымогательство, мошенничество и подделка.

Следует отметить, что сейчас государство находится в процессе совершенствования законодательства о киберпреступлениях. В конце 2015 г. была выпущена Национальная политика в об-

[1] The Critical Infrastructure Protection Act № 8, 2019. URL: https://www.gov.za/documents/critical-infrastructure-protection-act-8-2019-english-isixhosa-28-nov-2019-0000 (дата обращения: 20.01.2021).

[2] The Electronic Communications and Transactions Act № 25, 2002. URL: https://www.gov.za/documents/electronic-communications-and-transactions-act (дата обращения: 20.01.2021).

ласти кибербезопасности[1], за которой последовали проекты закона о киберпреступности и кибербезопасности[2].

Положения законопроекта раскрывают широкий круг киберпреступлений: незаконное обеспечение доступа, незаконное получение данных, незаконные действия в отношении программного или аппаратного обеспечения, незаконное вмешательство в данные или компьютерную программу, незаконное вмешательство в компьютерный носитель данных или компьютерную систему, незаконное получение, владение, предоставление, получение или использование пароля, кодов доступа и др.

Таким образом, в каждой стране есть свои особенности в установлении уголовной ответственности за киберпреступления. Чтобы эффективно противодействовать киберпреступности на межгосударственном уровне, БРИКС желательно принять единый документ, который содержал бы общее понимание киберпреступлений и их видов.

Р.А. Забавко,
доцент кафедры уголовного права Юридического института Иркутского государственного университета, кандидат юридических наук

О готовности российского уголовного права к использованию искусственного интеллекта при квалификации преступлений

Искусственный интеллект, лишенный многих ограничений человеческого разума, эффективно решает различные задачи не только в науке, иных высокотехнологичных отраслях, но и в тех сферах, где, как считалось долгое время, принимать решения может только человек. Все более распространенными становятся

[1] The National Cybersecurity Policy Framework for South Africa. № 609, 2015. URL: http://cybercrime.org.za/docs/National_Cybersecurity_Policy_Framework_2012.pdf (дата обращения: 20.01.2021).
[2] The Cybercrimes and Cybersecurity Bill, 2017. URL: https://www.gov.za/documents/cybercrimes-and-cybersecurity-bill-b6b-2017-7-nov-2018-0000 (дата обращения: 20.01.2021).

системы, которые способны воспринимать образы, обучаться (в том числе самостоятельно), обрабатывать огромные массивы данных. Искусственный интеллект не устает, не может быть предвзятым и не имеет корыстных или иных мотивов, может легко корректироваться, гораздо реже, чем человек ошибается. Несмотря на то что относительно ограничений, которые регулировали бы применение искусственного интеллекта в современном обществе, по-прежнему нет единой позиции, все это делает его привлекательным для решения правовых задач, в том числе связанных с квалификацией преступлений, и принятия иных решений, связанных с действием уголовного права.

Уже сейчас реализуются образовательные и научные проекты, в которых искусственный интеллект решает задачи правовой оценки, обрабатывает большие массивы юридической информации, принимает на основе изученного правовые решения, которые затем сравниваются с ранее вынесенными судами и правоохранительными органами: при решении относительно простых правовых задач специальные программы практически не ошибаются, а в общей массе всех рассмотренных ими дел точность превышает 70%. Некоторые крупные западные юридические компании активно используют компьютерные решения в качестве правовых помощников, в задачи которых входят обработка информации, интерпретация и систематизация данных, принятие юридических решений, которые в дальнейшем рассматриваются субъектами квалификации как рабочие версии.

Следует отметить, что в отечественном уголовном праве проблемы использования искусственного интеллекта как субъекта квалификации практически не поднимаются, основная масса ученых озабочена вопросами его правосубъектности и правовой оценки в качестве средства, орудия или способа совершения преступления. Отдельные исследования проводятся с позиции уголовно-процессуального права, так как именно процессуалисты знают, что принятие правового решения по своей сути – обработка больших массивов информации, выполнение задач анализа, сравнения, синтеза, производимые в узких рамках процессуальных норм[1].

---

[1] *Михайлов А.А.* Будущее уголовного процесса: прогностическое или реальное правосудие // Правовые проблемы укрепления российской государственности. сб. ст.; науч. ред. О.И. Андреева, Т.В. Трубникова. Томск: ИДУ ТГУ, 2018; *Осипов А.Л.* Междуна-

Вместе с тем проблема применения ресурсов искусственного интеллекта для правовой оценки содеянного и вынесения решений по делу материальная и относится к сфере действия уголовного права и квалификации преступлений. Наука квалификации преступлений, имеющая хорошо проработанные теоретические основы в российском праве, уже давно подготовила основательную базу для будущей автоматизации процесса квалификации преступлений[1]. В то же время многие проблемы не решены и могут стать существенным препятствием на пути использования искусственного интеллекта в уголовном праве.

Первый блок проблем связан с технико-юридическими недостатками уголовного законодательства и норм, к которым отсылают бланкетные диспозиции статей Особенной части УК РФ.

Так, уголовный закон из кодифицированного нормативного правового акта превратился в разрозненный документ, комплексное понимание которого затруднено многочисленными исключениями и специальными правовыми механизмами. Постоянное совершенствование уголовного законодательства при отсутствии генеральной стратегии или хотя бы руководящих начал правотворческой деятельности привело к тому, что многие нормы не соотносятся и необоснованно конкурируют друг с другом.

Все чаще законодатель, криминализуя конкретные деяния, не пользуется положениями Общей части УК РФ и даже не соотносит новеллы с ними. Огромное количество правовых фикций, созданных без особой нужды, привело к размыванию некоторых уголовно-правовых терминов. Так, содержание таких терминов, как «террористическое сообщество», «экстремистское сообщество», используемых в Особенной части УК РФ, не соотносится с понятием «преступное сообщество», предусмотренным ч. 4 ст. 35 УК РФ.

Некоторые правовые механизмы, играющие ключевую роль при определении преступности конкретных деяний, не имеют теоретико-правовых оснований в Общей части УК РФ. Например,

---

родно-правовые стандарты цифровизации уголовного судопроизводства и защита прав личности // Рос. правовая система в условиях четвертой промышленной революции: материалы VI Моск. юрид. форума, М.: Проспект, 2019 и др.

[1] См.: *Кудрявцев В.Н.* Общая теория квалификации преступлений. 2-е изд., перераб. и доп. М., 2004; *Кузнецова Н.Ф.* Проблемы квалификации преступлений: лекции по спецкурсу «Основы квалификации преступлений» / науч. ред. и предисл. акад. В.Н. Кудрявцева. М.: ИД «Городец», 2007 и др.

не понятна правовая природа примечания к ст. 122 УК РФ, где идет речь об освобождении от уголовной ответственности в связи с согласием потерпевшего на причинение ему вреда (которое, кстати, большинством авторов признается как не имеющее значения в вопросах уголовной ответственности), с одной стороны, и определенными действиями виновного – с другой.

В Общей части УК РФ размыты критерии многих важных правовых конструкций – малозначительности, обстоятельств, исключающих преступность деяния, назначения наказания и т.д.

Еще одна проблема – полисемия и омонимия терминологии в уголовном законодательстве. Одни и те же термины часто имеют совершенно иное значение. Так, термин «деяние» применяется и как характеристика всего содеянного, и как обязательный признак объективной стороны (это особенно актуально в составах с административной преюдицией, где появляется третье «деяние», признаки которого предусмотрены статьями КоАП РФ и которые называются законодателем «аналогичными»). В тексте УК РФ можно встретить упоминание о «фактически совершенном деянии» и о «деянии, предусмотренном конкретным составом преступления», которые имеют совершенно различное наполнение.

Есть в УК РФ проблемы с пониманием и таких терминов, как «вина», «виновный» (причем этот термин иногда трансформируется в «лицо, признанное виновным»), «потерпевший», «транспортное средство», «угроза» и т.д.

В связи с этим необходима масштабная реформа уголовного законодательства, которая обеспечила бы применение в тексте УК РФ слов в их общеупотребительных значениях, системное использование уточняющих терминов, законодательное толкование наиболее важных уголовно-правовых терминов.

Следующий блок проблем связан с наличием неразрешенных проблем конкуренции уголовно-правовых норм. К сожалению, в правоприменительной практике нередки случаи диаметрально противоположных решений, выносимых разными правоохранительными органами (в зависимости от территории или структуры). В принципе такие вопросы должны решаться Верховным Судом Российской Федерации и часто решаются, но не всегда оперативно, порождая ситуации правовой неопределенности.

С деятельностью Верховного Суда Российской Федерации связана еще одна проблема – он не всегда оперативно дает руководящие разъяснения по многим преступлениям и правовым ситуациям. Это часто объясняется формированием практики решения конкретных спорных ситуаций, однако иногда (например, при изменении норм УК РФ и смежного законодательства) от него требуется быстрая реакция.

Другая проблема – несовершенство законодательства, к которому отсылают бланкетные диспозиции статей Особенной части УК РФ или их примечания. Например, постановление Правительства Российской Федерации от 29.12.2018 № 1730 «Об утверждении особенностей возмещения вреда, причиненного лесам и находящимся в них природным объектам вследствие нарушения лесного законодательства» не может применяться для целей квалификации преступления, предусмотренного ст. 191^1 УК РФ. Другого нормативного правового акта, в котором содержались бы таксы и методики, необходимые для квалификации этого преступления, нет. В связи с этим деяния в обороте заведомо незаконно заготовленной древесины фактически декриминализованы.

Еще один блок проблем связан с уголовно-процессуальным правом. Многие системы искусственного интеллекта основаны на анализе больших массивов данных, способны воспринимать образы, систематизировать, сравнивать их и принимать определенные решения. Нужно отметить, что большинство программных решений в странах Запада работает на этом принципе. В российской правовой действительности такие программы работать не смогут, так как далеко не во всех приговорах судов первой инстанции, а особенно в решениях судов апелляционной, кассационной и надзорной инстанций, содержится истина в уголовно-правовом, материальном понимании. Решения судами часто признаются правовыми в тех случаях, когда они устраивают все стороны и достигнут критерий их неотменяемости.

Сказанное позволяет сделать вывод о том, что отечественное уголовное право к использованию искусственного интеллекта при квалификации преступлений фактически не готово.

А.В. Клочкова,
заведующий лабораторией
социально-правовых исследований
и сравнительного правоведения
юридического факультета МГУ
имени М.В. Ломоносова,
кандидат социологических наук

Влияние цифровой среды на формирование девиантного поведения подростков и молодежи

В Программе фундаментальных научных исследований в Российской Федерации на долгосрочный период (2021–2030 годы), утвержденной распоряжением Правительства Российской Федерации от 31.12.2020 № 3684-р, в качестве одного из основных направлений выделяется изучение влияния сети «Интернет», цифровых технологий на формирование криминологического статуса отдельных социальных групп и личности. В рамках этой задачи наиболее актуальным является акцентирование внимания на возрастной группе подростков и молодежи как наиболее подверженной негативному влиянию информационно-телекоммуникационных сетей.

Генетика задает вектор развития ребенка, определенную предрасположенность как к физическим и интеллектуальным возможностям, таланту, так и к асоциальному поведению. И насколько будет реализована данная предрасположенность, зависит в первую очередь от социума в целом, микросреды, а также от влияния цифровой среды в современном мире. В XXI в. традиционные воспитательные функции семьи, игравшие основополагающую роль в социализации детей на протяжении веков, значительно элиминированы воздействием информационно-телекоммуникационных сетей. Сеть вытеснила и межличностные связи, живое общение, в значительной степени обезличив социальную коммуникацию. Данная тенденция усугубилась в период пандемии. И если ранее основную информацию население черпало из печатных книг и телерадиопередач с позитивным контентом, художественная литература, изучаемая в школе, учила нравственно-

сти, благородству, ответственности, доброте, взаимопомощи, то в современном мире нельзя говорить о системе развития и интериоризации в сознании школьников традиционных ценностей, так как литература для значительного числа учеников сводится в прочтению краткого содержания произведений великих русских писателей, а обучение писать сочинение до 2014 г. было исключено из школьной программы. То есть уже не первое поколение воспитывается главным образом на телекоммуникационном информационном потоке, если не низвергающем традиционные морально-нравственные ориентиры, то, по крайней мере, не актуализирующем их в качестве основополагающего фундамента человеческого общежития.

По словам психиатра Андрея Курпатова, с ментальной точки зрения, «мы то, какую информацию мы потребляем»[1], а извлекается из сети «Интернет» тот контент, который может заинтересовать, к которому имеется склонность. В период пандемии, определенной ограниченности в передвижении, общении подросткам не хватает драйва, эмоций, экстрима, и они ищут выход в виртуальном пространстве, куда переместились коммуникационные связи. Здесь же сосредоточена информация, обладающая разрушительной для детской психики силой (приносящая вред здоровью и развитию детей и подростков).

По данным репрезентативных исследований, российские дети до 10 лет 40% времени проводят онлайн, в 14–18 лет данный объем времени увеличивается до 60%[2]. Цифровая среда становится жизненно важной для подростков, социальные сети, информационные и развлекательные порталы превращаются в неотъемлемую часть ежедневного времяпрепровождения. Виртуальный мир привлекает иллюзорной свободой и независимостью, снятием тех запретов, которые существуют в реальной жизни, своей значимостью для «друзей» или подписчиков. При этом большое число «друзей» в социальных сетях не гарантирует отсутствие одиночества в реальной жизни. Интернет-зависимость часто тесно связана с внутренним дискомфортом и дисгармонией подростка к концу подросткового периода. Либо появляется апа-

[1] *Курпатов А.* Идет эпидемия цифрового аутизма. URL: https://pravoslavie.fm/discussion/psihiatr-andrej-kurpatov-idyot-epidemiya-czifrovogo-autizma/ (дата обращения: 19.02.2021).
[2] Там же.

тия, пропадает интерес к жизни, либо, наоборот, актуализируется желание совершать все более рискованные поступки, получать больше адреналина, что является благоприятной почвой для интернет-манипулирования поведением подростка через агрессивное влияние на его сознание. Психологи предупреждают: опасность в том, что дети сами становятся жертвами своей неосмотрительности и неосторожности, так как способность к осознанной саморегуляции формируется у подростков к 14–15 годам[1], т.е. когда большинство из них уже все свое свободное время проводят в сети. По заключению специалистов в области психиатрии и психотерапии, в результате агрессивного воздействия виртуального пространства мы получаем к окончанию подросткового периода более половины психологически неблагополучных молодых людей, характеризующихся внутренней напряженностью, повышенной агрессивностью, низкой удовлетворенностью жизнью, социальной настороженностью, у которых чаще развиваются депрессивные состояния и появляются суицидальные наклонности[2].

Большинство представителей современной молодежи «переносят созданные в виртуальном мире нормы на реальные социальные отношения, тем самым разрушая сложившиеся нормативные устои общества, которые за последние десятилетия и так сильно деформированы, а их виртуализация приводит к еще большей деформации социального сознания и поведения»[3]. Реальная жизнь переходит в виртуальную, становится средой обитания, где не работают социальные законы, нарушаются социальные границы, отсутствует эмпатия, обесценивается внутренний мир человека.

Согласно результатам проведенного нами в 2018 г. криминологического исследования правосознания и ценностно-нормативных ориентаций студентов московских и региональных

---

[1] *Дозорцева Е.Г. и др.* Медицинская и судебная психология. М., 2016. С. 42.

[2] *Курпатов А.* Трансформация человека в цифровую эпоху: доклад в Совете Федерации. URL: http://council.gov.ru/events/news/113499/ (дата обращения: 18.02.2021).

[3] *Первушкин М.И., Юдина Е.С.* Эра киберсоциализации: роль интернета в социализации современной молодежи // Модели, системы сети в экономике, технике, природе и обществе. 2013. № 2. С. 238.

университетов[1], 34,3% опрошенных однозначно продемонстрировали ориентацию на общение в социальных сетях в ущерб межличностным контактам. Еще около трети (28,6%) респондентов склоняются к данному выбору. Таким образом, практически 2/3 студенческой аудитории отдают предпочтение интернет-взаимодействию, т.е. социальные коммуникации молодежи все больше трансформируются в виртуальные и переносятся в онлайн-пространство.

Устойчивой тенденцией становятся нежелание и неумение молодых людей поддерживать длительный психологический контакт друг с другом, утрата интереса к внутреннему миру друзей и близких, нивелирование ценности человеческих отношений. Как следствие, допущение промискуитета, непостоянства дружеских и интимных связей. Так, по мнению каждого второго опрошенного нами студента, молодежная культура подразумевает частую смену сексуальных партнеров (48,0%), что приводит к разводам, воспитанию детей в неполных семьях, их безнадзорности, интернет-зависимости, возрастанию рисков аддиктивного и иного девиантного поведения.

Специалисты Центра изучения и сетевого мониторинга молодежной среды определили около 30 субкультур, которые представляют потенциальную угрозу для подростков[2]. К ним в первую очередь следует отнести «группы смерти», сообщества, распространяющие идеи насилия и криминального образа жизни. С одной стороны, в виртуальное пространство шагнуло насилие из реальной жизни (кибербуллинг), с другой – оно само является источником насилия (в том числе аутонасилия), его реализации через вовлечение подростков в деструктивные сообщества. Сеть «Интернет», используемая деструктивными сообществами как механизм для продвижения в общественное сознание, и в первую очередь в сознание молодежи, своих идей, в настоящее время яв-

---

[1] Исследование правосознания студенческой молодежи проведено лабораторией социально-правовых исследований и сравнительного правоведения юридического факультета МГУ имени М.В. Ломоносова. Методика исследования – анкетирование. Выборка (866 человек) – студенты МГУ, МГЮА, Томского ГУ, Красноярского ГУ, Бурятского ГУ, РГГУ, Тимирязевской академии.

[2] *Почему* подростки вступают в субкультуры. URL: https://www.gazeta.ru/tech/2019/02/15_a_12185557.shtml. (дата обращения: 15.02.2021).

ляется прямым проводником в криминальную деятельность (распространение наркотиков, шоплифтинг, фродинг и т.д.).

Неотъемлемой составляющей цифровой социализации становится столкновение в той или иной степени с киберагрессией. Исследователями выделяются несколько видов сетевого буллинга. Большая часть подростков сталкивались в социальных сетях с флеймингом, троллингом и хейтингом[1]. По данным научных исследований, 15% детей становятся жертвами кибербуллинга с фиксированными деструктивными последствиями для психики ребенка: депрессивные, тревожные состояния, употребление психоактивных веществ, психосоматические заболевания, суицидальное поведение[2]. Основные риски киберпространства для детей и подростков состоят в опасности развития медиазависимости, деструктивном медиаконтенте, негативно виртуальном знакомстве, психическом насилии и угрозах, связанных с причинением вреда здоровью.

Ускорение развития технологий в телекоммуникационной сфере способствует интенсификации внедрения деструктивного контента в киберпространство, появлению новых девиантных течений с разрушительной составляющей. Данное обстоятельство, а также недостаточность изучения криминологических последствий негативного воздействия цифровой среды на сознание и поведение подростков и молодежи требуют акцентирования внимания специалистов на данной проблеме. Возросшие риски информационной безопасности детско-юношеской интернет-аудитории диктуют необходимость организации комплексных междисциплинарных криминолого-психолого-психиатрических научных исследований механизмов деструктивного воздействия информации, распространяемой посредством информационно-телекоммуникационной сети «Интернет» на формирование ценностно-нормативных ориентаций и установок девиантного поведения несовершеннолетних.

---

[1] *Солдатова Г.У., Рассказова Е.И., Чигарькова С.В.* Виды киберагрессии: опыт подростков и молодежи // Нац. психол. журн. 2020. № 2 (38).

[2] *Бочавер А.А., Докука С.В., Сивак Е.В., Смирнов И.Б.* Использование социальных сетей в интернете и депрессивная симптоматика у подростков // Клиническая и специальная психология. 2019. Т. 8. № 3. С. 2.

П.В. Никонов,
доцент кафедры Иркутского
юридического института (филиала)
Университета прокуратуры
Российской Федерации,
кандидат юридических наук,
доцент

Роль информационно-коммуникационных технологий и компьютерной информации в совершении коррупционных преступлений, связанных с дачей и получением взятки и иными видами незаконного вознаграждения

Развитие современного общества, обусловленное широким распространением информационно-коммуникационных технологий, их проникновением практически во все сферы жизни, привело к значительным трансформациям преступности, связанной с дачей и получением взятки и иными видами незаконного вознаграждения. Преступники получили новые способы коммуникации, осуществления взаиморасчетов, позволяющие им повысить свою криминальную активность и существенно снизить риски быть обнаруженными. Это, в свою очередь, требует адекватной реакции законодателя, который должен учитывать потенциал действующего УК РФ, уточнять общественную опасность отдельных деяний, корректировать содержание предмета, способа, средств совершения преступления.

В связи с этим представляется актуальным анализ сложившейся ситуации в части использования информационно-коммуникационных технологий и компьютерной информации в совершении коррупционных преступлений, связанных с дачей и получением взятки и иными видами незаконного вознаграждения, в целях совершенствования правового регулирования уголовной ответственности за их совершение.

Одной из проблем, с которой столкнулось общество, стало использование цифровой валюты (криптовалюты) для осуществления расчетов при совершении рассматриваемых преступлений.

В Российской Федерации основы правового регулирования обращения криптовалюты установлены в Федеральном законе от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации», большинство положений которого начало действовать только с 1 января 2021 г. Согласно п. 3 ст. 1 данного Федерального закона «цифровой валютой признается совокупность электронных данных (цифрового кода или обозначения), содержащихся в информационной системе, которые предлагаются и (или) могут быть приняты в качестве средства платежа, не являющегося денежной единицей Российской Федерации, денежной единицей иностранного государства и (или) международной денежной или расчетной единицей, и (или) в качестве инвестиций и в отношении которых отсутствует лицо, обязанное перед каждым обладателем таких электронных данных, за исключением оператора и (или) узлов информационной системы, обязанных только обеспечивать соответствие порядка выпуска этих электронных данных и осуществления в их отношении действий по внесению (изменению) записей в такую информационную систему ее правилам».

Использование криптовалюты привлекательно для преступного мира – это связано с ее сущностью, невозможностью отслеживания совершаемых с ее использованием транзакций, децентрализованной эмиссией, высокой стоимостью и универсальностью как средства платежа[1]. Использование криптовалюты при совершении рассматриваемых преступлений является дополнительным препятствием для организации их расследования и раскрытия, так как затрудняет оценку предмета преступления, наложение на него ареста, конфискации имущества и т.д.[2]

Предмет взяточничества и иных коррупционных преступлений составляют деньги, ценные бумаги, иное имущество либо незаконные оказание услуг имущественного характера, предоставление иных имущественных прав (ст. 290–291[2], 184, 200[5], 200[7],

---

[1] *Самолысов П.В.* Правовое регулирование майнинга криптовалют // Право и цифровая экономика. 2020. № 3.

[2] *Перов В.А.* Проблемные вопросы, возникающие при расследовании уголовных дел о преступлениях с использованием криптовалюты // Рос. следователь. 2020. № 7.

204–204[2] УК РФ). В ст. 141[1] УК РФ предметом преступления выступают денежные средства, материальные ценности, товары, оказание платных услуг. Анализ каждого из указанных видов позволяет прийти к выводу о том, что отнесение криптовалюты к одному из них является затруднительным в силу ее особой правовой природы и связанной с этим возможности определения ее имущественной ценности. Формально криптовалюту можно отнести к иным имущественным правам. Несмотря на то что криптовалюта является официально установленным средством платежа, легальный механизм определения ее стоимости не регламентирован. С учетом правовой позиции, выраженной в постановлении Пленума Верховного Суда Российской Федерации от 09.07.2013 № 24 «О судебной практике по делам о взяточничестве и об иных коррупционных преступлениях», обязывающей доказывать стоимость предмета взятки, отсутствие сведений об этом исключает возможность безусловного ее признания предметом данного преступления, как и преступлений, предусмотренных п. «а» ч. 2 ст. 141, ч. 2 ст. 142, ч. 1 ст. 183, ч.1 и 4 ст. 309 УК РФ. Даже несмотря на то что там он обозначен как подкуп, его содержание на практике фактически ограничено содержанием предмета взяточничества и иных коррупционных преступлений, связанных с незаконным вознаграждением.

Не решают проблемы и некоторые попытки Пленума Верховного Суда Российской Федерации учитывать реальный криминогенный потенциал криптовалюты, предпринятые им в обновленной редакции постановления от 07.07.2015 № 32 «О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем», в котором криптовалюта обозначена в качестве предмета преступлений, предусмотренных ст. 174 и 174[1] УК РФ (в случае, если она преобразована в денежные средства). Вместе с тем, как считают некоторые специалисты в области уголовного права, криптовалюта близка к денежным суррогатам, ко-

торые, в свою очередь, входят в предмет взяточничества и иных коррупционных преступлений, связанных с подкупом[1].

Сказанное привело к тому, что реально имеющие повышенную общественную опасность деяния не могут быть квалифицированы как преступления, связанные с дачей и получением взятки и иными видами незаконного вознаграждения. Вместе с тем из ситуации есть выход – признать криптовалюту предметом данных преступлений. Однако дальнейшее развитие информационно-коммуникационных технологий может привести к появлению новых предметов, которые могут быть использованы при осуществлении расчетов в коррупционных целях. Включение криптовалюты, например в ч. 1 ст. 290 УК РФ, и признание ее предметом подкупа при совершении иных коррупционных преступлений проблему в корне не решает. В связи с этим предлагаем признавать предметом коррупционных преступлений, связанных с дачей и получением взятки и иными видами незаконного вознаграждения, любые блага (в том числе и нематериальные), которые стимулируют публичное должностное лицо к совершению преступления. Это позволит признать предметом рассматриваемых преступлений не только криптовалюту, но и иные предметы (услуги, права, блага), появление которых возможно вследствие технического прогресса.

Вторая проблема связана с использованием информационно-коммуникационных технологий для совершения самого общественно опасного деяния – коррупционных преступлений, связанных с дачей и получением взятки и иными видами незаконного вознаграждения.

Дифференциация уголовной ответственности предполагает учет при криминализации, установлении наказания и иных мер уголовно-правового воздействия на виновного, которые влияют на характер и степень совершенного им деяния. Использование возможностей современных средств коммуникации в качестве средств достижения и реализации соглашения о передаче предмета взятки или иного коррупционного преступления, связанного

---

[1] *Огородникова Н.В., Коновалов А.К.* Отражение прогресса информационных технологий в содержании УК РФ (на примере законодательного определения предмета взятки) // Юрид. вестн. Кубан. гос. ун-та. 2020. № 4.

с подкупом, а также выполнения публичным должностным лицом действий в пользу дающего подкуп или иного лица существенно повышает возможности виновных лиц оказывать негативное воздействие на охраняемые законом общественные отношения, оставаясь скрытыми от внимания правоохранительных органов. В связи с тем, что для достижения и реализации договоренности, осуществления расчетов при применении информационно-коммуникационных технологий виновным не требуется личного контакта, существенно расширяется территория криминального рынка коррупционных услуг.

Все это требует реакции со стороны законодателя. Думается, наиболее адекватной мерой реагирования государства на существенно повысившуюся общественную опасность коррупционных преступлений, связанных с дачей и получением взятки и иными видами незаконного вознаграждения, станет введение квалифицированных составов этих преступлений, в которых было бы дополнительно криминализовано использование электронных или информационно-телекоммуникационных сетей, в том числе сети «Интернет», как способа и средств преступления.

Полагаем, что признание в качестве предмета коррупционных преступлений, связанных с дачей и получением взятки и иными видами незаконного вознаграждения, криптовалюты и вообще любых благ (в том числе нематериальных), а также введение квалифицирующего признака «с использованием электронных или информационно-телекоммуникационных сетей, в том числе сети «Интернет» в составы этих преступлений позволит устранить образовавшиеся вследствие технического прогресса правовые пробелы и значительно повысить уровень противодействия коррупции в стране.

М.А. Соколов,
заместитель заведующего
лабораторией НИИ
Университета прокуратуры
Российской Федерации,
кандидат юридических наук

Медиасреда как фактор криминализации молодежи

Современные комплексные криминологические исследования, основанные в том числе на достижениях социологии и психологии по вопросу возрастных пределов молодежного возраста, позволяют сделать вывод о том, что молодежный возраст находится в пределах 18–29 лет. При этом ранний молодежный возраст, т.е. период жизни человека от 18 до 24 лет, является во многом определяющим. Несмотря на достижение совершеннолетия, в этом возрасте все еще не происходит окончательного приобретения всей полноты качеств, свойственных взрослым людям, а по своим социальным и психологическим характеристикам представители этой возрастной группы демонстрируют значительное сходство с аналогичными характеристиками несовершеннолетних.

Одной из особенностей рассматриваемой возрастной группы является то, что молодежь отличается стремлением к образованию неформальных групп, в том числе антисоциальной направленности, что значительно ускоряет процесс распространения на их участников деструктивного влияния и вовлечения в преступную деятельность.

Важными в контексте рассматриваемого вопроса являются такие криминологические характеристики молодежи, как оценка ее в качестве наиболее криминально пораженной части населения страны, преступники данной возрастной группы готовы для достижения своих корыстных целей к применению насилия, опасного для жизни или здоровья.

В силу отсутствия необходимого жизненного опыта, достаточного уровня образования, приемлемого социального статуса, возможности реализоваться в предпринимательской деятельности, а также иных характеристик, позволяющих совершать более «интеллектуальные» и «прибыльные» преступления, лица раннего молодежного возраста представляют интерес для организован-

ных преступников своими физическими данными (угрожающим внешним видом, силой и др.), а также наличием определенных навыков, которые они успели приобрести к данному возрасту (умение управлять автомобилем, обращаться с оружием и т.д.).

Обладая указанными качествами, лица 18–24 лет чаще всего включаются в преступную деятельность, связанную с совершением насильственных преступлений. В данном случае они представляют собой своеобразное орудие преступления в силу того, что являются лишь исполнителями отведенной им роли.

Безусловно, такая восприимчивость молодежи дает возможность криминально ориентированным лицам и их группам использовать представителей 18–29-летнего населения страны в деструктивных целях.

При отсутствии необходимого социального контроля и предлагаемых социальной средой позитивных альтернатив, позволяющих разрушить негативные социальные связи, поведение лица раннего молодежного возраста подвергается активной криминализации со стороны организованных преступников.

Одним из инструментов отмеченной криминализации является размещение в медиасреде соответствующих информационных материалов. При этом под медиасредой понимается сфера, которая через посредничество массовых коммуникаций (печать, радио, ТВ, видео, кино, компьютерные каналы, сеть «Интернет» и т.д.) связывает человека с окружающим миром, информирует, развлекает, пропагандирует те или иные нравственно-эстетические ценности, оказывает идеологическое или организационное воздействие на мировоззрение и социальное поведение людей. Важно отметить, что информационные материалы, и прежде всего о криминальной субкультуре, распространяемые в сети «Интернет», оказывают серьезное влияние на криминализацию поведения молодежи путем формирования у нее преступной мотивации.

Следует отметить, что организованные преступные формирования представляют собой своеобразные социальные институты криминального характера. Длительность их существования выразилась в формировании своеобразной криминальной субкультуры как совокупности определенных норм поведения внутри своей среды.

Проведенные исследования свидетельствуют о том, что криминальная субкультура способствует осуществлению организованной преступной деятельности, ее формирование является одним из основных направлений преступной самоорганизации, предполагая целенаправленное распространение норм и традиций своей среды[1].

По сути, успешное распространение криминальной субкультуры, особенно в подростково-молодежной среде, обеспечивает не только длительное совершение широкого перечня преступлений, но и бесперебойное пополнение состава организованных преступных формирований новыми участниками, которые продолжают совершать преступления.

Пока индивид находится в рамках таких общностей, успешность его социализации определяется принятыми в них правилами и образцами. Сконструированные в автономных социальных общностях (признаваемых в обществе в одних случаях нормальными, в других – девиантными) групповые ценности и нормы выступают для их членов важнейшими жизненными ориентирами, которые позволяют отделить своих от чужих сформировать свой взгляд на мир и человека[2].

В этом случае воздействие организованной преступности на конкретную личность носит не прямой, а опосредованный характер, когда непосредственное воздействие на лицо, в том числе молодого возраста, не осуществляется, но оно знает о наличии различных организованных преступных формирований и сознательно допускает для себя возможность участия в их деятельности.

Распространение криминальной субкультуры может иметь и неумышленную форму. При этом криминологические аспекты вовлечения гораздо шире уголовно-правовых, поскольку неумышленное распространение преступной романтики не может повлечь уголовно-правовых последствий. Однако подражание авторитетному лицу с криминальным прошлым может привести к преступным результатам[3].

---

[1] *Соколов М.А.* Молодежь в системе криминальной репродукции: монография. М.: Юрлитинформ, 2018.

[2] *Луков Вал. А.* Теории молодежи: междисциплинарный анализ: науч. монография. М.: Канон+ РООИ «Реабилитация», 2012. С. 370.

[3] *Криминология:* учебн. для студентов вузов, обучающихся по специальности Юриспруденция / под ред. Г.А. Аванесова. М.: ЮНИТИ-ДАНА, 2013. С. 250.

В немалой степени формированию соответствующей мотивации способствуют некоторые произведения современного искусства, романтизирующие, а нередко и оправдывающие преступный образ жизни, навязывающие молодежи необоснованно завышенные материальные потребности. Исследователями отмечается ведущая роль средств массовой информации в распространении криминальной субкультуры, влияние которых сопровождается вытеснением семьи и образовательных организаций на вторые позиции[1].

Криминологи указывают на взаимосвязь между молодежной преступностью и интенсивностью распространения средствами массовой информации материалов, дезориентирующих значительную часть молодежи в отношении социальных ценностей и жизненных планов[2].

Как показывает изучение материалов уголовных дел, серьезный мотивирующий эффект имеет то обстоятельство, что организованные преступные формирования осуществляют своеобразную социальную поддержку своих членов и их семей: в случае гибели, ранения либо привлечения к уголовной ответственности. Немаловажным фактором является предоставляемое содействие в достижении желаемого материального благополучия, реализации жизненных планов. Практика принятия внутри криминального сообщества подобных мер способствует укреплению позиций криминальной субкультуры и увеличивает число ее сторонников.

Контраст между социальной невознаграждаемостью законопослушного поведения и социальной успешностью, основанной на криминале, стимулирует маргинализированную часть молодежи на реализацию своих потребностей посредством криминальной деятельности, переориентировав свое поведение на нормы криминальной субкультуры. На этой почве происходит сближение криминальной и молодежной субкультур[3].

В силу распространенности у молодежи фрустрации, являющейся следствием начала самостоятельной жизни после достижения совершеннолетия, представляется, что именно лица раннего

---

[1] *Психологическая* устойчивость молодежи к негативным социальным влияниям: монография / под ред. Е.И. Середа. Псков: Гименей, 2010. С. 355; *Самыгин П.С.* Правовая социализация учащейся молодежи в условиях социальной неопределенности российского общества: автореф. … дис. д-ра социол. наук. Ростов н/Д., 2008. С. 23.

[2] *Варчук Т.В.* Криминология: учеб. пособие. М.: ИНФРА-М, 2002. С. 174.

[3] *Самыгин П.С.* Указ. соч. С. 21.

молодежного возраста в наибольшей степени подвержены негативному воздействию криминальной субкультуры.

Следует также подчеркнуть, что формирование необоснованно завышенных потребностей и интересов, а также во многом и преступной мотивации в значительной мере происходит под воздействием массовой информации. Эта информация является важным инструментом создания и расширения криминальной субкультуры, что при сложившемся уровне информационных технологий делает негативное воздействие на личность тотальным.

Отмечая наличие подобной причинно-следственной связи, в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов граждан Российской Федерации, обеспечения безопасности государства необходимо законодательно установить запрет на распространение сведений о нормах поведения в криминальной среде, средствах коммуникации, используемых ее представителями, а также информации, направленной на оправдание организованной преступной деятельности в различных ее проявлениях.

Несмотря на имеющиеся в действующем законодательстве инструменты противодействия распространению негативной информации, следует отметить необходимость комплексного подхода к регулированию в том числе контрольной (надзорной) деятельности в области информационно-телекоммуникационных сетей, зачастую являющихся не только способом, но и в каком-то смысле местом совершения противоправных действий. В связи с этим целесообразно принятие федерального закона, предусматривающего все аспекты такой деятельности.

Как представляется, безусловный приоритет при построении системы противодействия рассматриваемому негативному явлению должен иметь комплексный криминологический подход, предусматривающий общие и специальные меры по профилактике противоправного поведения, включающий меры социального, экономического и воспитательного характера.

О.В. Пристанская,
старший научный сотрудник,
заместитель директора Ассоциации
участников рынка интернет-индустрии
«Лига безопасного интернета»,
кандидат юридических наук

Совершенствование законодательства в сфере противодействия кибербуллингу и другим видам психологического насилия в отношении несовершеннолетних посредством сети «Интернет»

С развитием современных средств связи и массовых коммуникаций все более широкие масштабы приобретает культивирование в социальных сетях насильственных и иных антиобщественных моделей выстраивания межличностных отношений и разрешения конфликтов, проявления кибертравли и других видов насилия с использованием информационно-телекоммуникационных сетей. Так, согласно аналитическому отчету Крибрум[1], по состоянию на сентябрь 2019 г. под влиянием деструктивного контента находились 39,2 млн аккаунтов, в том числе 7 млн аккаунтов подростков, активному деструктивному воздействию подвергалось 45% от общего числа подростков в России. В кибербуллинг вовлечены более 12 млн пользователей (из них 2,5 млн подростков). При этом численность несовершеннолетних участников интернет-сообществ «буллеров» и «троллей» на протяжении ряда лет стабильно составляет около 2,5 млн человек.

Проведенный в ходе исследования включенности подростков в интернет-пространство и их отношения к кибербуллингу (2017–2019 гг.) [2] анонимный опрос 44 учеников 8-х классов в возрасте 13–15 лет показал, что практически все (97%) опрошенные подростки сталкивались с кибербуллингом, причем большинство

---

[1] Анализ распространения деструктивного поведения молодежи в социальных медиа. Аналитический отчет. Период исследования: 01.09.2017 – 15.09.2019. Подготовлен Крибрум 19.09.2019. См. также: О форуме «Цифровая гигиена. URL: http://digital-gigiena.ru/.

[2] *Дозорцева Е.Г., Кирюхина Д.В.* Кибербуллинг и склонность к девиантному поведению у подростков // Прикладная юрид. психология. 2020. № 1(50).

(56%) использовали интернет-травлю в качестве ответа на агрессию. Формы кибербуллинга, которым подверглись подростки: издевательство – 77%, раскрытие личной информации – 51%, травля (диссинг) – 48%, киберпреследование – 39%, троллинг – 31% опрошенных.

Кибернасилие проявляется в разнообразных формах[1], причиняющих существенный вред чести, достоинству, репутации, здоровью, нравственному, духовному, психическому и физическому развитию несовершеннолетних. По оценкам экспертов, жертвы кибербуллинга испытывают серьезные психологические, психосоматические, социальные и поведенческие проблемы (высокий уровень тревоги, суицидальные мысли, депрессия, агрессивное поведение, употребление алкоголя и других психоактивных веществ, трудности в социализации)[2].

Не менее опасны набирающие популярность в социальных сетях, в том числе среди несовершеннолетних[3], так называемые

---

[1] Высмеивание и моральное подавление ребенка (в мировой практике обозначаемое термином «кибертроллинг»); его преследование с целью запугивания угрозой противозаконных действий или повреждений, доведения до паники и отчаяния посредством систематической рассылки угрожающих, вызывающих тревогу и раздражение сообщений (кибersталкинг); систематическая упорная травля в сети «Интернет», распространение в социальных сетях информации, порочащей честь и достоинство жертвы (кибербуллинг); совращение ребенка непристойными сообщениями и изображениями, склонение к ведению сексуальных разговоров, провоцирование к отправке сексуальных фото-, видеоматериалов, сексуальный шантаж, распространение в сети непристойных эротических и порнографических изображений жертвы (секстинг, интернет-груминг); размещение видеосюжетов со сценами побоев, истязаний и иных насильственных действий в отношении детей и подростков (хеппислепинг); размещение негативных комментариев и сообщений, иррациональной критики в адрес конкретного человека или явления (хейтинг); вспышки оскорблений в ходе публичного эмоционального обмена репликами в чатах и комментариях в социальных сетях (флэйминг); преследование игроками других игроков в многопользовательских онлайн-играх с целью лишить удовольствия от игры (грифинг) и др.

[2] См.: *Дозорцева Е.Г., Кирюхина Д.В.* Указ. соч.; *Perren S.* et al. Bullying in School and Cyberspace: Associations with Depressive Symptoms in Swiss and Australian; *Campbell M.* Victims' Perceptions of Traditional and Cyberbullying, and the Psychological Correlates of their Victimisation // Emotional and Behavioural Difficulties. 2012. Vol. 17, iss. 3, no. 1. P. 389, 398 и др.

[3] Так, по итогам 2019 г. ежемесячно российские пользователи только приложения TikTok просматривали в среднем 16,25 млрд и размещали 20,83 млн видео; делились 23 млн и ставили лайки 1,62 млрд видео (Is Time Against TikTok? - GlobalWebIndex; GlobalWebIndex Blog; TikTok раскрыл данные по просмотрам видео в России).

треш-стримы[1], сопровождающиеся употреблением в прямом эфире алкогольных напитков и иных психоактивных веществ, нецензурной бранью, драками, издевательствами над избранными жертвами, истязаниями, нанесением увечий, склонением к совершению действий, причиняющих вред жизни и здоровью самих жертв и других лиц.

Повышенная общественная опасность насилия и жестокости в сети «Интернет» в значительной мере обусловлена доступностью, массовым характером, многообразием форм и высокой интенсивностью обмена информацией в виртуальном пространстве, анонимностью пользователей, отсутствием жесткой регламентации сетевого поведения, прозрачностью границ. Указанная проблема обостряется в период самоизоляции и санитарно-эпидемиологических ограничений, введенных в связи с пандемией новой коронавирусной инфекции.

Особого внимания и контроля со стороны государства требует размещение в сети «Интернет» видеосюжетов со сценами побоев, истязаний и иных насильственных действий в отношении детей и подростков, что способствует культивированию насилия и провоцирует на подобные съемки[2]. В Доктрине информационной безопасности Российской Федерации повышение эффективности профилактики и противодействия правонарушениям, совершаемым с использованием информационных технологий, выделяется в качестве одного из основных направлений обеспечения государственной и общественной безопасности[3].

В то же время системный анализ федерального законодательства показывает, что оно охватывает не все виды и формы кибернасилия, направленного против несовершеннолетних, не учитывает их высокой общественной опасности, не содержит необходимых правовых гарантий предупреждения их негативного

---

[1] Онлайн-трансляции, в которых любой пользователь (в том числе постоянные подписчики) в обмен на финансовые подарки, пожертвования (так называемые донаты) может наблюдать, как ведущий-стример бьет или унижает другого человека, так называемого контентмейкера, выполняющего унизительные и жестокие задания (челленджи) зрителей и сносящего разного рода физические и психические испытания.

[2] Концепция развития системы профилактики безнадзорности и правонарушений несовершеннолетних на период до 2025 года, утв. распоряжением Правительства РФ от 22.03.2017 № 520-р.

[3] Утв. Указом Президента РФ от 05.12.2016 № 646.

влияния на честь, достоинство, репутацию, здоровье и развитие детей. С целью устранения правовой пробельности в этой сфере необходимо разработать и принять комплекс законодательных мер, направленных на обеспечение эффективного мониторинга, выявления, предупреждения и пресечения разных видов насилия и жестокости, совершаемых с использованием электронных и информационно-телекоммуникационных сетей, и введение повышенной административной и уголовной ответственности за их совершение в отношении детей и подростков.

Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» следует дополнить следующими нормами. Дополнить перечень видов информации, запрещенной для распространения среди детей, информацией, «содержащей угрозы, шантаж, оскорбления, клевету или иные сведения, унижающие человеческое достоинство ребенка или его близких» (п. 7^1 ч. 2 ст. 5). Указать, что в целях ограничения доступа детей к сайтам в сети «Интернет», содержащим информацию, причиняющую вред их здоровью и развитию, запрещенную для распространения в Российской Федерации, сведения о таких сайтах вносятся в Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено в порядке, предусмотренном ст. 15^1 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ч. 4 ст. 14).

Соответственно, предусмотренный Федеральным законом «Об информации, информационных технологиях и о защите информации» перечень видов информации, подлежащей включению в названный Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов на основании решений уполномоченных Правительством Российской Федерации федеральных органов исполнительной власти, следует дополнить «информацией, направленной на систематическое причинение несовершеннолетнему психических страданий путем запугивания, шантажа, угроз, публичных оскорблений или публичного распространения иной информации, унижающей челове-

ческое достоинство потерпевшего или его близких» (подп. «и» п. 1 ч. 5 ст. 15[1]).

В Федеральном законе от 24.07.1998 № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации» необходимо отнести к целям государственной политики в интересах детей защиту детей от факторов, негативно влияющих не только на их развитие, но и на здоровье, в том числе в информационно-телекоммуникационных сетях (новая редакция абз. 5 ч. 1 ст. 4); «обеспечение безопасности жизни и здоровья детей и их информационной безопасности, в том числе при пользовании информационно-телекоммуникационными сетями» (абз. 6 ч. 1 ст. 4). В п. 1 ст. 14 следует учесть все виды информации, запрещенной для распространения среди детей в соответствии с ч. 2 ст. 5 Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию», в том числе распространяемой в информационно-телекоммуникационных сетях, включая сеть «Интернет».

В Федеральном законе от 24.06.1999 № 120-ФЗ «Об основах системы профилактики безнадзорности и правонарушений несовершеннолетних»: 1) дополнить определение понятия «антиобщественные действия» указанием на возможность совершения действий, нарушающих права и законные интересы других лиц, «с использованием электронных и информационно-телекоммуникационных сетей, включая сеть «Интернет» (абз. 6 ст. 1); 2) уточнить перечень основных задач деятельности по профилактике безнадзорности и правонарушений несовершеннолетних в части выявления и пресечения случаев вовлечения несовершеннолетних в совершение преступлений, других противоправных и антиобщественных действий, а также склонения их к суицидальным действиям указанием на возможность совершения таких действий «с использованием электронных и информационно-телекоммуникационных сетей, включая сеть «Интернет» (п. 1 ст. 2); 3) расширить и уточнить полномочия органов и учреждений системы профилактики безнадзорности и правонарушений несовершеннолетних, отнеся к ним обязанности: осуществлять защиту несовершеннолетних от всех форм дискриминации, физического или психического насилия, оскорбления, грубого обращения, сексуальной и иной эксплуатации, совершаемых с использо-

ванием информационно-телекоммуникационных сетей, включая сеть «Интернет»; незамедлительно информировать орган внутренних дел о несовершеннолетних, в отношении которых совершены противоправные деяния либо которые совершили правонарушение или антиобщественные действия с использованием информационно-телекоммуникационных сетей, включая сеть «Интернет»; незамедлительно информировать орган по делам молодежи о выявлении фактов распространения в информационно-телекоммуникационных сетях, включая сеть «Интернет», информации, склоняющей или иным способом побуждающей детей к совершению действий, представляющих угрозу их жизни и здоровью, а также жизни и здоровью иных лиц, для внесения сведений о таких электронных ресурсах в Единый реестр в порядке, предусмотренном ст. 15^1 Федерального закона «Об информации, информационных технологиях и о защите информации» (п. 2 ст. 14); 4) дополнить обязанностью «обеспечивать защиту в образовательных организациях несовершеннолетних обучающихся (воспитанников) от информации, причиняющей вред их здоровью и развитию, в том числе распространяемой с использованием информационно-телекоммуникационных сетей, включая сеть «Интернет», полномочия организаций, осуществляющих образовательную деятельность (подп. 6 п. 2 ст. 14).

В Федеральном законе от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»: 1) дополнить ч. 5 ст. 16 обязанностью организаций, осуществляющих образовательную деятельность, обеспечивать «защиту несовершеннолетних обучающихся (воспитанников) от информации, причиняющей вред их здоровью и развитию, при реализации образовательных программ с применением электронного обучения, дистанционных образовательных технологий; 2) перечень основных академических прав обучающихся, установленный ч. 1 ст. 34, дополнить правом на информационную безопасность (п. 9); 3) перечень гарантируемых государством мер охраны здоровья обучающихся, установленных ч. 1 ст. 41, дополнить пропагандой и обучением навыкам не только здорового, но и безопасного образа жизни, в том числе навыкам информационной безопасности при пользовании информационно-телекоммуникационными сетями, включая сеть «Интернет» (п. 4), а также обеспечением информационной безопасности

обучающихся во время пребывания в организации, осуществляющей образовательную деятельность (п. 8).

В Кодекс Российской Федерации об административных правонарушениях внести следующие изменения: 1) ввести признак совершения административного правонарушения «в информационно-телекоммуникационных сетях, включая сеть «Интернет», в квалифицированный состав оскорбления, предусмотренный ч. 2 ст. 5.61, а также в ч. 3 ст. 5.61, устанавливающую административную ответственность за непринятие мер к недопущению оскорбления, совершенного публично; 2) ввести ст. 5.61[1] «Унижение человеческого достоинства несовершеннолетнего», включающую несколько составов административных правонарушений, объединяемых общим родовым объектом: а) распространение в электронных или информационно-телекоммуникационных сетях, включая сеть «Интернет», любых сведений, порочащих честь и достоинство несовершеннолетнего или подрывающих его репутацию (за исключением заведомо ложных сведений, охватываемых действием ст. 128[1] УК РФ), либо иной информации, которая оскорбляет человеческое достоинство несовершеннолетнего, если эти действия не содержат уголовно наказуемого деяния; б) несистематическое причинение несовершеннолетнему психических страданий путем запугивания, шантажа, угроз, публичных оскорблений или публичного распространения иной информации, унижающей человеческое достоинство потерпевшего или его близких, если эти действия не содержат уголовно наказуемого деяния; в) непринятие мер к недопущению распространения указанной в настоящей статье информации о несовершеннолетнем в электронных или информационно-телекоммуникационных сетях, включая сеть «Интернет», лицами, на которых возложены такие обязанности в силу их служебного положения или профессиональной деятельности[1]; г) фото- или видеосъемка совершения уголовно наказуемых деяний против здоровья (умышленного причинения вреда здоровью разной степени тяжести, побоев, истязания, угроз убийством или причинением тяжкого вреда здоровью), чести и достоинства (клевета), половой неприкосновенно-

[1] Аналогичный состав административного правонарушения предусмотрен ч. 3 ст. 5.61 КоАП (Оскорбление).

сти, совершенных в отношении несовершеннолетних, в целях шантажа потерпевших или публичной демонстрации созданных таким образом фото-, видеоматериалов в электронных или информационно-телекоммуникационных сетях, включая сеть «Интернет», направленная на причинение психических страданий потерпевшему, если эти действия не содержат уголовно наказуемого деяния.

В Уголовном кодексе Российской Федерации предлагаем дополнить части вторые ст. 111 (Умышленное причинение тяжкого вреда здоровью), 112 (Умышленное причинение средней тяжести вреда здоровью), 115 (Умышленное причинение легкого вреда здоровью), 116 (Побои), 116^1 (Нанесение побоев лицом, подвергнутым административному наказанию), 117 (Истязание), 119 (Угроза убийством или причинением тяжкого вреда здоровью), 128^1 (Клевета) квалифицирующим признаком, отражающим повышенную общественную опасность публичной демонстрации актов физического и психического насилия, в том числе в электронных или информационно-телекоммуникационных сетях[1], особенно в случаях, когда такие деяния совершаются в отношении несовершеннолетних[2].

В целях предупреждения и пресечения попыток совращения ребенка в режиме онлайн с целью его последующей сексуальной эксплуатации в сети «Интернет» или в реальной жизни ч. 2 ст. 133 (Понуждение к действиям сексуального характера) и ч. 2 ст. 135 УК РФ (Развратные действия) следует дополнить квалифицирующим признаком «с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет».

Предлагаем также ввести в УК РФ ст. 151^3 (Травля несовершеннолетнего), предусматривающую уголовную ответственность за систематическое причинение несовершеннолетнему психических страданий путем запугивания, шантажа, угроз, пуб-

---

[1] Такой же квалифицирующий признак содержится в ст. 205^2 (Публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма) и ст. 280^1 (Публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации).

[2] Аналогичный квалифицирующий признак предусмотрен п. «г» ч. 2 ст. 245 УК РФ, устанавливающей уголовную ответственность за жестокое обращение с животными.

личных оскорблений или публичного распространения иной информации, унижающей человеческое достоинство или порочащей честь и достоинство потерпевшего или его близких. Выделить в качестве квалифицирующего признака данного деяния его совершение с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет». Выделить особо квалифицированный состав данного преступления, предусматривающий причинение вреда здоровью потерпевшего, психическое расстройство несовершеннолетнего или иные тяжкие последствия.

Считаем также необходимым ввести в УК РФ ст. 151^4 (Организация публичной травли несовершеннолетнего в электронных или информационно-телекоммуникационных сетях, включая сеть «Интернет»): 1) предусматривающую уголовную ответственность за организацию деятельности, направленной на систематическое публичное распространение в электронных или информационно-телекоммуникационных сетях, включая сеть «Интернет», информации, содержащей угрозы, шантаж, оскорбления, или иной информации, унижающей человеческое достоинство несовершеннолетнего или его близких с целью причинения потерпевшему психических страданий; 2) предусматривающую в качестве квалифицирующих признаков причинение вреда здоровью, психическое расстройство несовершеннолетнего или иные тяжкие последствия; 3) устанавливающую, что лицо, совершившее преступление, предусмотренное данной статьей, добровольно прекратившее соответствующую преступную деятельность и активно способствовавшее раскрытию и пресечению преступлений, предусмотренных ст. 151^3 и 151^4 УК РФ, освобождается от уголовной ответственности, если в его действиях не содержится иного состава преступления[1].

В Уголовно-процессуальный кодекс Российской Федерации (подп. «а» п. 1 ч. 2 ст. 151) предлагается внести изменения, направленные на отнесение преступлений, предусмотренных

[1] Аналогичная норма предусмотрена ст. 110^2 УК РФ (Организация деятельности, направленной на побуждение к совершению самоубийства) и позволяет привлекать к уголовной ответственности лиц, организовавших травлю несовершеннолетних в виртуальных сетях.

ст. 151^3, 151^4 УК РФ, к подследственности следователей Следственного комитета Российской Федерации.

Концепция законопроекта соответствует направленности современной государственной политики России на приоритетную защиту государством семьи, материнства и детства, в том числе отраженную в Конституции Российской Федерации с изменениями, одобренными в ходе общероссийского голосования.

П.Н. Фещенко,
заведующий кафедрой
уголовного права и криминологии
Волго-Вятского института (филиала)
Университета имени О.Е. Кутафина
(МГЮА), кандидат юридических
наук, доцент

К вопросу о личности «цифрового преступника» и его жертвы

Рассматривая преступность как негативное социально-правовое явление, криминологи пришли к выводу о ее прямой зависимости от происходящих в обществе изменений. При этом, в частности, развитие техники и технологий как повышает эффективность борьбы с преступностью через создание банков информации, систем идентификации личности и т.д., так и способствует совершению преступлений через облегчение доступа к конфиденциальной информации, обезличенному контакту с жертвами и т.п.

Как показывает статистика, в последние годы при общем снижении регистрируемой преступности компьютерные преступления демонстрировали постоянный рост, что можно рассматривать как свидетельство высокого профессионализма преступников и наличия постоянного большого количества виктимного (доверчивого) населения.

Как отметил Министр внутренних дел Российской Федерации В. Колокольцев на ежегодном расширенном заседании коллегии МВД 26 февраля 2020 г., сотрудниками полиции «повышен-

ное внимание уделялось выявлению, раскрытию и расследованию преступлений, совершаемых с использованием информационно-коммуникационных технологий… Рост криминальных деяний данного вида оказал значительное влияние на динамику и структуру преступности в целом. Их доля в общем массиве достигла почти 15 процентов и продолжает расти»[1].

Подтвердила негативную тенденцию и ситуация с карантинными ограничениями. Как указывают в своем исследовании Н.Р. Шевко и Э.Р. Рафикова, «введение строгих мер самоизоляции в апреле 2020 года привело к значительному спаду т.н. уличной преступности.

Наибольшее снижение наблюдалось по следующим группам преступлений – изнасилования и покушения на изнасилование – на 31,1%; разбои – на 20,9%; кражи – на 11,2%; грабежи – на 9,9%.

При этом число преступлений с использованием интернет-технологий возросло на 93,2%, мобильных технологий – на 97,7%»[2].

Говоря о причинах этого явления, авторы указывают, что «введение режима самоизоляции перевело работу большей части населения в виртуальное пространство при низком уровне информационной безопасности, что повлекло утечку данных, несанкционированный доступ к конфиденциальной информации и др. При этом среди физических лиц весомую часть пострадавших от киберпреступности составляют либо люди преклонного возраста, не способные противостоять психологическим приемам в столь экстремальных условиях и с недостаточным уровнем компьютерной грамотности, либо дети и подростки, для которых Интернет, социальные сети стали единственным доступным способом общения»[3].

---

[1] Заседание коллегии МВД России. URL: http://kremlin.ru/events/president/transcripts/62860 (дата обращения: 05.01.2021).

[2] *Шевко Н.Р., Рафикова Э.Р.* Преступность в период пандемии COVID-2019 как угроза национальной безопасности // Реакция государства на преступное поведение, уголовно-правовое воздействие и уголовная ответственность в системе мер обеспечения национальной безопасности: сб. материалов круглого стола, г. Тольятти, 24 нояб. 2020 г. / редкол. В.Д. Дуюнов, Р.В. Закомолдин; Ин-т права Тольяттинского гос. ун-та. Самара, 2020.

[3] Там же. С. 68.

Прежде всего, на наш взгляд, в качестве проблемы следует выделить особенность личности «цифрового преступника». Это человек, которого специалисты-педагоги обучили премудростям работы с современной техникой или способам влияния на людей, – это выпускники вузов, получившие дипломы «компьютерщиков», «психологов», «специалистов по управлению персоналом». Это люди, тщательно планирующие преступления и подбирающие жертв, не наркоманы и алкоголики, не нищие и бездомные, не закончившие даже среднюю школу. У них есть современная техника, и они годами живут на криминальные доходы.

С позиции подходов криминологии к исследованию личности преступника, можно сказать, что их всех объединяет этап социализации – их не воспитали в духе уважения к Закону, чужой собственности, не сформировали личность с качеством сострадания, которая никогда не взяла бы у бедного пенсионера последние деньги с электронной карточки… И коль скоро таких «высокообразованных» преступников становится все больше и больше, проблему можно считать относящейся ко всей системе современного образования.

Признанием неблагополучной ситуации можно считать внесенные не так давно Президентом Российской Федерации инициативы – дополнения в Федеральный закон «Об образовании», которые в СМИ, как представляется, совершенно правильно назвали Законом о воспитании[1].

Как отметил председатель Госдумы Вячеслав Володин, «образование должно включать не только знания и навыки, но и духовные, моральные ценности, которые формируют личность, объединяют общество»[2].

В то же время понятно, что результаты такого воспитательного процесса дадут положительный эффект только в отдаленной перспективе, когда выпускники школ и вузов выйдут во «взрослый мир» и будут для себя решать вопрос, каким путем получать средства для существования – честным трудом или через крими-

---

[1] *Госдума* приняла президентский закон о воспитании в школах и вузах. URL: https://rg.ru/2020/07/22/gosduma-priniala-zakon-o-vospitanii-obuchaiushchihsia.html (дата обращения: 05.01.2021).

[2] Там же.

нализацию полученных знаний, в том числе в сфере компьютерных технологий.

При этом уже сегодня можно усилить виктимологическую профилактику, сосредоточив активность правоохранительных органов и СМИ на разъяснении уловок интернет-мошенников, что и делается сегодня в широких масштабах, включая размещение соответствующих материалов на сайтах МВД, прокуратуры и иных ведомств[1].

Проблема в том, что жертвами оказываются как раз те, кто эти сайты не посещает, рекомендации не изучает и наивно верит всему, что ему говорят «представители банков» по сотовой связи. На наш взгляд, это проблема одиноких пожилых людей, решить которую можно, в частности, через систему адресного просвещения, в том числе с использованием волонтеров.

Автор еще помнит, как в конце 1990-х гг. в Федеральной программе профилактики преступности на очередные 5 лет был пункт, предусматривавший выявление всех одиноких собственников квартир и проверку фактов, если они вдруг лишились этой собственности. Это и был реальный шаг в направлении адресной работы с виктимным населением. Сегодняшняя криминальная статистика дает основания сделать вывод, что пока мошенники с такой категорией населения работают более эффективно, получая разными путями конфиденциальную личную информацию о составе семьи, номерах телефонов, наличии денег на счете и т.д. и т.п.

---

[1] В частности, на сайте УМВД России по Кировской области в разделе «Противодействие мошенничеству» размещены актуальные материалы о преступниках и их жертвах: «В отношении кировчанки совершено дистанционное мошенничество в особо крупном размере (30.12. 2020); «Более 13 миллионов рублей лишились кировчане за неделю, поверив дистанционным преступникам» (29.12.2020); «Дистанционные мошенники обманом похитили у кировчанки более 1 миллиона рублей» (29.12.2020) и т.д. URL: https://43.мвд.рф/news/rubric/5680/ (дата обращения: 05.01.2021).

В Интернете размещены многочисленные материалы профилактического характера, например: «Внимание! Мошенничество в Интернете!». URL: http://vemst.ru/punkt-menyu; «Виды мошенничеств в сетях сотовой и проводной связи и в сети Интернет». URL: https://74.мвд.рф/профилактика-мошенничества; «Профилактика мошенничеств, совершаемых в сети Интернет и с помощью сети Интернет». URL:https://vk.com/@policevufal-profilaktika-moshennichestv-sovershaemyh-v-seti-internet-i-s и т.д. (дата обращения: 05.01.2021).

Важным в плане противодействия, на наш взгляд, является общий для всех так называемых интеллектуальных преступлений, а также профессиональной и организованной преступной деятельности вопрос о возможности безбедно и долго жить на преступные доходы, не вызывая вопросов ни у правоохранительных органов, ни у граждан, которые в последние десятилетия стали разобщены и эгоистичны.

Как показывают материалы уголовных дел, интернет-мошенники зачастую хорошо организованы, имеют офисы и дорогостоящую технику и годами совершают преступления, ни перед кем не отчитываясь об источниках доходов[1].

На наш взгляд, к положительным аспектам в попытках решить данную проблему следует отнести все чаще появляющуюся информацию о намерениях властей решить вопрос о контроле за теневыми доходами через контроль расходов всех слоев населения[2].

Подводя итог, можно сделать вывод о том, что государственные планы и программы цифровизации общества создадут еще большее поле деятельности для киберпреступников, при этом снизить рост преступности в компьютерной сфере можно целенаправленной системой мер, включающих совершенствование правового и нравственного воспитания граждан, адресную виктимологическую профилактику, а также затруднение возможности безбедно жить на преступные доходы, что является не столько проблемой криминологической теории, сколько задачей повышения качества деятельности законодателей, представителей правоохранительных органов и педагогического сообщества.

---

[1] *Приговоры* судов по ст. 159 УК РФ Мошенничество. URL:https://advocate-service.ru/sud-praktika/ugolovnye-dela/prigovory-sudov-po-st.-159-uk-rf-moshennichestvo.html и др. (дата обращения: 05.01.2021).

[2] *Минэкономразвития* предложило ввести контроль над расходами россиян. URL: https://www.rbc.ru/economics/27/06/2019/5d14b6c09a79473f652b8fcc и др. (дата обращения: 05.01.2021).

Е.Г. Маныч,
доцент юридической кафедры
Московского инновационного
университета, кандидат
юридических наук

Кража финансовых данных или данных банковских карт – один из видов киберпреступления

Мы живем в век информационных технологий, которые позволили человечеству сделать прорыв во многих научных сферах. Информационные технологии развиваются со стремительной силой и, конечно же, как любое явление, имеют как позитивные, так и негативные последствия. Но человечество уже не сможет существовать без информационных технологий, поэтому мы должны учитывать все негативные последствия и предупреждать их.

Понятие «киберпреступление» появилось с развитием информационных технологий. Киберпреступление – это, прежде всего, преступная деятельность, цель которой незаконное использование компьютера и компьютерной сети. Многие киберпреступления совершаются хакерами (киберпреступники, которые таким образом зарабатывают деньги). Киберпреступления могут осуществляться как физическим лицом, так и организацией. С каждым годом киберпреступники находят все новые и новые способы совершения киберпреступлений.

Выделяют несколько типов киберпреступлений[1]:

1) мошенничество с электронной почтой и интернет-мошенничество;
2) мошенничество с использованием личных данных;
3) кража финансовых данных или данных банковских карт;
4) кража и продажа корпоративных данных;
5) кибершантаж;
6) атаки программ-вымогателей;
7) криптоджекинг (криптовалюта с использованием чужих ресурсов без согласия владельца);
8) кибершпионаж.

[1] Kaspersky.ru

Кража финансовых данных или данных банковских карт в России является одним из самых распространенных видов киберпреступлений.

Такие киберпреступления совершаются по разным схемам: мошенник звонит конкретному (физическому) лицу, представляясь при этом сотрудником банка, и под разными уговорами, предложениями пытается выяснить у своей жертвы срок действия карты, CVC-код банковской карты, а также логин и пароль от мобильного банка.

Очень часто мошенники не звонят своим жертвам, но денежные средства снимаются, могут уйти в другой регион. При этом не происходит никакого оповещения на телефон владельца банковской карты, и даже сотрудники банка не в курсе, что деньги незаконным путем сняты или перечислены на другую банковскую карту. Обнаруживается кража денежных средств, когда владелец банковской карты приходит в банк, чтобы снять денежные средства. Нередко, к сожалению, это бывают пенсионные начисления, которые пришли на банковскую карту. Распространены случаи, когда владелец банковской карты, посетив банк для того, чтобы положить денежные средства на счет банковской карты, не подозревает, что при выходе из банка у него автоматически снимутся денежные средства. Сотрудники банка, проводя свое небольшое расследование, могут узнать, в какой регион ушли денежные средства и на какую организацию были перечислены данные средства. Вероятность вернуть денежные средства владельцу мала.

Схемы краж финансовых данных или данных банковских средств постоянно меняются и совершенствуются мошенниками.

Сегодня основной защитой от мошенничества может быть предупреждение данного вида киберпреступления, а именно постоянная осведомленность граждан, которые обслуживаются в банке (при оформлении банковской карты выдавать памятки пользователя о мерах безопасности, отправлять периодически SMS-сообщения о мерах безопасности).

Предупреждение кражи финансовых данных или банковских карт заключается, прежде всего, в следующем:

1) не сообщать никому пароль, логин от мобильного банка, а также CVC-код банковской карты, срок действия карты;

2) использовать такие пароли, которые трудно подобрать;

3) не передавать свои личные данные по телефону, электронной почте, если не уверены;

4) если человек, который вам звонит, просит предоставить какие-либо ваши данные, то следует положить трубку, перезвонить в банк и рассказать о ситуации;

5) внимательно просматривать свои банковские выписки;

6) запоминать, какого числа и какую сумму вы сняли или перевели последний раз, если что-то покажется подозрительным, необходимо обратиться в банк для выяснения обстоятельств;

7) не нажимать на ссылки в спам-сообщениях (даже если оно пришло от банка, где вы обслуживаетесь, лучше перезвонить в банк и уточнить информацию).

Сегодня МВД России и Роскомнадзор совместно с Банком России и Генеральной прокуратурой Российской Федерации разрабатывают санкции за мошенничество под видом предоставления государственных выплат. Необходимость разработки плана борьбы с фишинговыми сайтами, а также специальных нормативных актов возникла из-за участившихся случаев, когда при переходе по ссылке мошеннический сайт просит ввести данные банковской карты для проверки права на выплату, после чего у владельца карты автоматически списываются денежные средства.

Информационные технологии совершенствуются, изменяются почти каждый день, соответственно и мошеннические схемы при совершении киберпреступлений совершенствуются и меняются. Поэтому очень важно создать специальную нормативную базу, которая позволила бы быстро реагировать на появление новых мошеннических схем киберпреступлений.

А.К. Клименко,
старший преподаватель кафедры
общеправовых дисциплин
Дальневосточного юридического
института МВД России

Проблемы квалификации хищений, совершенных с использованием технологии бесконтактной оплаты

Масштабное распространение информационных технологий в банковской сфере привело к появлению новых форм банковского обслуживания, новых электронных услуг и, как следствие, к колоссальному росту оборота безналичных и электронных денежных средств.

Стремительный рост безналичных и электронных денежных средств неизбежно способствовал тому, что последние все чаще становятся предметом преступных посягательств.

Сложившаяся ситуация определила внесение изменений в Уголовный кодекс Российской Федерации [1]. Так, ч. 3 ст. 158 и ч. 3 ст. 159^6 были дополнены особо квалифицирующим признаком «с банковского счета, а равно в отношении электронных денежных средств». Кроме того, изменена редакция ст. 159^3 УК РФ, в диспозиции которой указаны способ и средства совершения преступления – «с использованием электронных средств платежа». Данными изменениями расширены способ и предмет преступного посягательства, а также сняты ограничения по кругу лиц, участвующих в ходе совершения данного преступления и подвергающихся обману или злоупотреблению доверием.

К сожалению, к настоящему времени еще не выработана единообразная судебная практика по применению указанных квалифицирующих признаков.

Противоречивым образом сложилась практика при квалификации деяний, совершенных с использованием такого инновационного продукта, как технологии бесконтактной оплаты. Указанная услуга является одной из самых распространенных в силу

[1] Федеральный закон от 23.04.2018 № 111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации».

явных преимуществ – простоты, легкости в использовании, молниеносной скорости проведения заданной операции.

Технология бесконтактной оплаты активно совершенствуется, и теперь помимо банковских карт модулем NFC (Near field communication – ближняя связь без контакта) снабжаются такие гаджеты, как сотовый телефон, наручные часы, кольца, расширяя возможности данной технологии до практически безграничных. В будущем будут использоваться только бесконтактные способы оплаты, уверяют в ПАО «Сбербанк России»[1].

При квалификации хищений безналичных и электронных денежных средств, совершенных с использованием технологии бесконтактной оплаты, определяющее значение имеет наличие лица, предоставляющего терминал, или же его отсутствие, например на кассе самообслуживания. В последнем случае не возникает никаких противоречий при квалификации деяний, поскольку касса самообслуживания – «техническое устройство, лишенное психики не может находиться в состоянии заблуждения относительно предоставляемой информации, то есть классического обмана нет»[2], оплата товара похищенной или поддельной банковской картой происходит без участия уполномоченных лиц, т.е. хищение происходит тайно.

В случае же участия лица, предоставляющего терминал для оплаты покупок виновным по чужой банковской карте, сложилась противоречивая судебная практика, несмотря на прямое разъяснение в п. 2 и абз. 1 п. 17 постановления Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» о том, что действия виновного квалифицируются по ст. 159[3] УК РФ. К сведениям, о которых умалчивается при совершении преступления, отнесены любые обстоятельства, относящиеся к личности виновного, в рассматриваемом случае – умолчание перед работником торговой организации о факте использования платежной карты лицом, не являющимся ее истинным владельцем, т.е. ее незаконном использовании.

---

[1] *Как* отключить бесконтактную оплату. URL: https://www.sravni.ru/banki/info/kak-otkljuchit-beskontaktnuju-oplatu-sberbank/ (дата обращения: 05.01.2021).

[2] *Хилюта В.В.* Направленность мошеннического обмана на иных лиц: границы и содержание // Уголовное право. 2020. № 4.

Законодательные новеллы, расширившие границы электронного мошенничества (ст. 159^3 УК РФ), не только не оправдали ожидания законодателя, заключающиеся в очевидной квалификации преступлений, но и породили конкуренцию с электронной кражей (п. «г» ч. 3 ст. 158 УК РФ) ввиду разного толкования указанных уголовно-правовых норм. Как следствие – отсутствие единого подхода при квалификации подобных преступлений на протяжении двух лет со дня их принятия.

Так, анализ приговоров, постановлений судов первой инстанции, апелляционных представлений и определений, а также определений суда кассационной инстанции по данной категории дел показывает, что суды, обосновывая переквалификацию действий подсудимого (осужденного), оплачивавшего покупки платежной картой, не принадлежащей ему, с использованием технологии бесконтактной оплаты, путем прикладывания карты к считывающему устройству терминала, предоставляемого продавцом, приводили следующие доводы:

при обосновании квалификации деяния по ч. 2 (при значительном ущербе) ст. 159^3 УК РФ. «Бесконтактное хищение происходит обманным способом, поскольку, принимая во внимание положения абз. 1 п. 17 указанного постановления (в случае, когда хищение имущества осуществляется с использованием принадлежащей другому лицу расчетной или иной платежной карты путем умолчания уполномоченному работнику торговой или иной организации о незаконном владении им платежной картой), К. присутствующим работникам торговой организации умалчивает о незаконном владении банковской картой, тем самым обманывая их»[1], а продавец в силу положения п. 5 ст. 10 ГК РФ, «предполагая добросовестность участников гражданских правоотношений и разумность их действий»[2], не сомневается в правомочности действий лица, использующего не принадлежащую ему банковскую карту.

Кроме того, положение п. 4 постановления Пленума Верховного Суда Российской Федерации от 27.12.2002 № 29 «О судебной практике по делам о краже, грабеже, разбое» о том, что

---

[1] Архив Центрального районного суда г. Комсомольска-на-Амуре за 2018 г. Дело № 1-659/2018. Приговор от 11.10.2018.

[2] Апелляционное определение Хабаровского краевого суда от 11.12.2018 по уголовному делу № 22-3855/2018. URL: https://kraevoy--hbr.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=9448623&delo_id=4&new=4&text_number=1 (дата обращения: 05.01.2021).

хищение является тайным, когда присутствующее при незаконном изъятии чужого имущества лицо не сознает противоправность этих действий, не находит подтверждения в описываемых обстоятельствах дела, поскольку, по мнению суда, касается поведения лиц, которые не участвуют в незаконном изъятии имущества. В данном случае при совершении мошенничества продавец под влиянием обмана предоставляет считывающий терминал для продажи мошеннику выбранного им товара, выполняя тем самым активные действия, вовлекаясь таким образом в объективную сторону мошенничества[1];

при обосновании квалификации деяния по п. «в» ч. 3 ст. 158 УК РФ. На основании разъяснений п. 4 постановления Пленума Верховного Суда Российской Федерации от 27.12.2002 № 29, когда присутствующее при незаконном изъятии чужого имущества лицо не сознает противоправность этих действий, хищение признается тайным. Так, присутствующий работник торговой организации при оплате товара банковской картой с функцией бесконтактной оплаты не сознает незаконность изъятия имущества и обмана, поскольку не знает истинного владельца банковской карты, поэтому бесконтактное хищение происходит тайным способом в отсутствие потерпевшего[2].

Ни в одном нормативном правовом акте не установлено, что держатель банковской карты при проведении расчетов должен предъявлять документ, удостоверяющий личность. Таким образом, оплачивая покупки не принадлежащей лицу банковской картой, прикладывая ее к терминалу, предоставляемому сотрудником торговой организации без документа, удостоверяющего личность, владелец карты не обманывал сотрудника и не вводил его в заблуждение, хотя и умалчивал о своей личности[3].

Кульминационным моментом в квалификации хищений безналичных и электронных денежных средств, совершенных с использованием услуги бесконтактной оплаты в присутствии ли-

---

[1] Там же.

[2] Апелляционное постановление Свердловского областного суда от 02.04.2018 по уголовному делу № 22-2232/2018. URL: https://oblsud--svd.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=4700037&delo_id=4&new=4&text_number=1 (дата обращения : 05.01.2021).

[3] Там же.

ца, предоставляющего виновному терминал для оплаты, стала позиция Верховного Суда Российской Федерации, изложенная в определении по уголовному делу № 12-УДП20-5-К6[1]. Верховный Суд Российской Федерации усомнился в правильности квалификации действий виновного К. по ч. 3 ст. 30, ч. 1 ст. 159^3 УК РФ. К. нашел банковскую карту с функцией бесконтактной оплаты, принадлежащую другому лицу. После чего произвел оплату покупок на общую сумму 3026 руб. 54 коп. путем прикладывания банковской карты к терминалу, предоставляемому работником торговой организации, тем самым похитив указанные денежные средства.

В обоснование своей позиции Верховный Суд Российской Федерации опирается на три аргумента. Первый заключается в том, что работники торговой организации не принимают участия в осуществлении транзакции по списанию денежных средств с банковского счета при оплате товара, поэтому К. ложные сведения о принадлежности карты сотрудникам торговых организаций не сообщал и в заблуждение их не вводил. Второй довод состоит в том, что на работников торговых организаций, осуществляющих платежные операции, действующими нормативными актами не возлагается обязанность, заключающаяся в идентификации держателя карты по документам, удостоверяющим личность. Третий – применяемые к содеянному положения п. 17 постановления Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48, обусловливающие квалификацию по ст. 159^3 УК РФ (об умолчании о незаконном владении платежной картой), являются необоснованными, поскольку предназначались для старой редакции ст. 159^3 УК РФ, а не для ныне действующей, введенной Федеральным законом от 23.04.2018 № 111-ФЗ через пять месяцев после принятия Пленумом Верховного Суда Российской Федерации названного постановления.

Не согласимся с позицией Верховного Суда Российской Федерации, который расценил содеянное как мошенничество с использованием электронных средств платежа, а не как кражу, совершенную с банковского счета. Оппонируя первому аргументу,

---

[1] Определение суда кассационной инстанции (в порядке гл. 47^1 УПК РФ) от 29.09.2020 по уголовному делу № 12-УДП20-5-К6. URL: http://vsrf.ru/stor_pdf.php?id=1917106 (дата обращения : 05.01.2021).

согласимся с позицией краевого суда, что работник торговой организации, находясь в состоянии заблуждения относительно правомерности действий виновного, совершает активные действия, заключающиеся в предоставлении виновному терминала, чтобы последний расплатился[1].

Оспаривая второй аргумент, отметим, что и виновный совершает активные действия, по справедливому мнению В.В. Хилюты[2] и Ю.Ю. Малышевой[3], направленные на активный обман, заключающийся в предъявлении чужой карты (а также других гаджетов, снабженных модулем NFC: телефона, наручных часов, кольца и т.д.), указывая на свою правомочность на оплату приобретенных товаров. В свою очередь И.К. Клепицкий считает, что виновный совершает пассивный обман (путем бездействия), который возможен лишь при наличии обязанности совершить действие, поэтому очевидно, что работник торговой организации не может быть обманут. Учитывая, что работник торговой организации не может быть обманут, а также что последний не проверяет правомочия плательщика распоряжаться картой, И.К. Клепицкий сравнивает его с прохожим[4]. Однако роли прохожего и работника торговой организации не равны, поскольку именно без участия последнего, предоставляющего терминал для оплаты товаров, таким образом вовлеченного в объективную сторону хищения, снятие безналичных денежных средств со счета банковской карты в качестве оплаты товаров может не состояться, в отличие от прохожего, не участвующего в объективной стороне преступления. Из чего следует заключить, что, предъявляя чужую платежную карту, а также телефон и другие гаджеты, оснащенные модулем NFC, виновный показывает свою правомочность на пользование указанными средствами, а работник торговой организации безоговорочно в силу действия ст. 10 ГК РФ считает, что его действия являются добросовестными и разумными.

---

[1] Апелляционное определение Хабаровского краевого суда от 11.12.2018 по уголовному делу № 22-3855/2018 // Сайт Хабаровского краевого суда.

[2] *Хилюта В.В.* Указ. соч.

[3] *Малышева Ю.Ю.* Проблемы квалификации обмана как способа совершения мошенничества с использованием электронных средств платежа // Мониторинг правоприменения. 2018. № 4.

[4] *Клепицкий И.К.* Кража без денег: простой ответ на простой вопрос // Уголовное право. 2020. № 5.

Кроме того, указание Верховного Суда Российской Федерации на необоснованность применения п. 17 названного постановления, по нашему мнению, несостоятельно. Во-первых, потому, что постановление не отменено. Во-вторых, указание в постановлении на круг лиц, присутствующих при оплате товаров и подвергающихся обману, предусмотренных старой редакцией ст. 159^3 УК РФ, не меняет всей картины в квалификации.

Не соглашаясь с мнением И.К. Клепицкого о том, что Федеральный закон от 23.04.2018 № 111-ФЗ перевел ст. 159^3 УК РФ в разряд компьютерных, а также о том, что указание на «обман уполномоченного работника кредитной, торговой или иной организации» в первоначальной редакции ст. 159^3 УК РФ было анахронизмом, обоснуем свою позицию. По нашему мнению, законодатель обновил редакцию ст. 159^3 УК РФ, преследуя одну главную цель – цель борьбы с преступлениями, совершенными с использованием электронных платежных систем и сети «Интернет». Стремительное развитие информационно-коммуникационных технологий и применение их в финансовом секторе (интернет-банкинг, интернет-эквайринг) расширили спектр электронных услуг и удаленный доступ к счетам для совершения платежей и переводов. Учитывая факт динамично развивающихся технологий, опережающих создание эффективных механизмов права борьбы с преступностью, законодатель максимально расширяет применение диспозиции ст. 159^3 УК РФ. Именно для этого в диспозиции применяется термин «электронные средства платежа», подразумевающий согласно п. 19 ст. 3 Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе» осуществление перевода денежных средств в форме безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, в том числе платежных карт, а также иных технических устройств. А также снимаются ограничения по кругу лиц, подвергающихся обману и предоставляющих терминал для оплаты, участвуя, таким образом, в совершении преступления.

Из сказанного следует заключить, что внесенные в УК РФ Федеральным законом от 23.04.2018 № 111-ФЗ изменения нельзя признать состоявшимися, поскольку на протяжении двух лет отсутствует единая правоприменительная практика относительно рассматриваемых законодательных новелл.

К.В. Шевелева,
преподаватель кафедры
«Правовое обеспечение
национальной безопасности»
МИРЭА – Российского
технологического университета

Об ответственности за реабилитацию нацизма в сети «Интернет». Вопросы терминологии

Роль цифровых технологий в жизни общества в последние годы значительно выросла. Информационные технологии стали частью жизни практически каждого гражданина нашей страны. Так как IT-общество развивается стремительно, возросла угроза общественной безопасности в сети «Интернет». Информационная структура сети позволяет преступникам оставаться анонимными, действовать скрытно, осуществляя свою деятельность из любой точки мира. За последние несколько лет компьютерная преступность существенно трансформировалась и посягает на различные общественные отношения, в том числе и на историческую память народа Российской Федерации.

Правоохранительные органы вынуждены реагировать на эту ситуацию. 24 декабря 2014 г. гражданин В. опубликовал на личной странице в социальной сети «ВКонтакте» статью под названием «15 фактов о бандеровцах, или о чем молчит Кремль». Согласно статистике, публикацию увидели более 20 пользователей. Сотрудниками Следственного комитета Российской Федерации было возбуждено уголовное дело по ст. 354[1] УК РФ (Реабилитация нацизма). В материалах дела говорилось, что гражданин, совершив репост статьи, распространил заведомо ложные сведения о деятельности СССР в годы Второй мировой войны. В. стал первым обвиняемым по данной статье[1], поскольку норма введена в УК РФ Федеральным законом от 05.05.2014 № 128-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации». Всего же с момента введения данной статьи в Уголовный кодекс Российской Федерации осуждено более

[1] URL: https://fparf.ru/news/fpa/dvesti-tysyach-za-repost/ (дата обращения: 15.01.2021).

200 человек, из них 70% совершили деяния, подпадающие под объективные признаки преступления с использованием информационно-телекоммуникационных сетей[1].

По нашему мнению, в дальнейшем подобного рода правонарушения будут расти, и важно квалифицированно осуществлять правоприменительную практику на основе действующих юридических норм. Принятие решения зависит от умения профессионального субъекта осуществлять юридическое познание, убедительно аргументировать собственные суждения. В целях правильного толкования нормы и последующего решения, влекущего определенные правовые последствия, необходимо понимать смысл тех или иных слов (фраз), используемых в нормативных правовых актах нашей страны. В уголовном праве Российской Федерации реализация данного положения необходима в первую очередь для однозначного понимания содержания преступления, его сущности, а также объективных признаков, которые в дальнейшем будут влиять на уголовно-правовую квалификацию и назначение наказания.

В данном контексте обратим внимание на терминологию уголовного законодательства, касающуюся нашей темы. Статья 354[1] вводит в уголовное право важное понятие «реабилитация», но содержание статьи в настоящем виде не соответствует сущности понятия.

Рассмотрим этимологию понятия «реабилитация». Согласно Толковому словарю под реабилитацией понимается восстановление в правах, устранение последствий чего-либо[2].

Существует мнение, что исторически термин «реабилитация» возник в юридических и политических кругах европейских стран, США и Канады. Например, В.А. Бобренёв связывает его восхождение со средневековым французским институтом помилования осужденного, с восстановлением его прежних прав. По его мнению, впервые термин был употреблен французским легистом Блеймио[3].

В России понятие «реабилитация» получило широкое распространение после XX съезда КПСС (1956 г.), смысловое опре-

---

[1] URL: https://sledcom.ru/activities/statistic/ (дата обращения: 15.01.2021).
[2] Толковый словарь С.И. Ожегова//ozhegov.ru. (дата обращения: 13.01.2021).
[3] *Бобренёв В.А.* За отсутствием состава преступления. М., 1998. С. 86.

деление которого связывали с оправданием невинно репрессированных граждан и народов, полным восстановлением по суду или в административном порядке в социально-политических и гражданских правах, признанием репутации незапятнанной, снятием выговора, административного взыскания, судимости. Советское уголовное право определяло термин «реабилитация» как восстановление в прежнем состоянии невиновного лица, которое было привлечено к уголовной ответственности необоснованно[1].

В современной России термин «реабилитация» закреплен в Уголовно-процессуальном кодексе Российской Федерации. Так, в п. 34 ст. 5 УПК РФ под реабилитацией понимается «порядок восстановления прав и свобод лица, незаконно или необоснованно подвергнутого уголовному преследованию, и возмещения причиненного ему вреда». Глава 18 УПК РФ регламентирует основной процессуальный порядок восстановления в правах, устранение последствий имущественного и морального вреда. Уголовный процессуальный закон придает данному термину положительную окраску, выделяя восстановление в правах как основное действие, определяющее сущность данного понятия.

Таким образом, исходя из изученной нами этимологии анализируемого понятия сразу же возникает вопрос о смысловой нагрузке и применимости его для определения объективных признаков состава преступления, предусмотренного ст. 354[1] УК РФ. Ознакомление с содержанием данной статьи дает основание оспаривать употребление понятия «реабилитация» в названии, возможно, данный термин требует корректировки либо замены, для того чтобы передать точный смысл и значение состава преступления, охватываемого ст. 354[1] УК РФ.

В большей степени формулировка статьи обеспечивает охрану общественных отношений, связанных с решением Нюрнбергского трибунала, а также с исторической памятью о подвиге, совершенном советским народом. В то же время в Российской Федерации наблюдаются рецидивы нацистской идеологии, в том числе распространение нацистской символики и ценностей, например с использованием информационных технологий, что, в

[1] *Зак Г.Г.* Исторический анализ сущности понятия «реабилитация» в системе специального образования // Спец. образование. 2012. № 3.

свою очередь, неблагоприятно влияет на общественное и историческое сознание, способствует неверному толкованию исторических фактов и их фальсификации. Однако данные общественные отношения не охвачены детальным правовым регулированием.

Нарушение закона, запрещающего героизировать нацизм, распространять заведомо ложные сведения о деятельности СССР в военное и послевоенное время, а также ряд деяний, совершенных с целью выразить явное неуважение к общественной памяти, нашли выражение в объективной стороне рассматриваемого преступления:

1) отрицание фактов, установленных приговором Международного военного трибунала для суда и наказания главных военных преступников европейских стран оси, совершенное публично;

2) одобрение преступлений, установленных указанным приговором;

3) распространение заведомо ложных сведений о деятельности СССР в годы Второй мировой войны, совершенное публично;

4) распространение выражающих явное неуважение к обществу сведений о днях воинской славы и памятных датах России, связанных с защитой Отечества;

5) осквернение символов воинской славы России.

Анализируя практические аспекты деятельности органов предварительного расследования, осуществляющих квалификацию, а также устанавливающих обстоятельства, подлежащие доказыванию, можно сделать вывод о том, что им необходимо обращаться к приговору Нюрнбергского трибунала в целях избежания юридических ошибок. Так, Нюрнбергский трибунал устанавливает международно-правовую квалификацию действий Германии в Европе как виновника агрессивной войны, включающей в себя совершение преступлений против мира и безопасности человечества, выразившееся в том, что подсудимые, захватив правительственный контроль над Германией, планировали, подготавливали и вели агрессивные войны, которые являлись также войнами, нарушающими международные договоры, соглашения и обязательства.

Сравнивая юридические нормы, мы наблюдаем несоответствие действий, отражающих объективную сторону данного преступления, его названию. В положениях ст. 354^1 УК РФ отсутствуют сущностные признаки понятия «реабилитация», а именно восстановление кого-либо или чего-либо в правах, а также устранение последствий каких-либо явлений. Думается, законодатель имел в виду, скорее, информационно-пропагандистские и оценочные суждения в отношении роли СССР во Второй мировой войне, деяния по искажению и надругательству над символами воинской славы России.

Сомнение вызывает и целесообразность введения в ст. 354^1 УК РФ ч. 3, так как в норме не конкретизируются исторические периоды, подпадающие под распространение сведений, выражающих явное неуважение к обществу о днях воинской славы и памятных датах России, связанных с защитой Отечества, а также не раскрыто понятие «символы воинской славы», осквернение которых, в свою очередь, влечет уголовную ответственность. Следовательно, возникает вопрос, идет ли речь лишь о Нюрнбергском наследии либо данная статья охватывает более широкую сферу общественных отношений.

Таким образом, можно сделать вывод о том, что значение понятия «реабилитация» в ст. 354^1 УК РФ не соответствует содержательной части объективной стороны преступления, что, в свою очередь, может внести путаницу в правоприменительную практику, а именно в определение конкретных деяний, которые служат основанием для привлечения к уголовной ответственности по данной статье. Для того чтобы норма действительно работала, на наш взгляд, необходимо внести изменение в название статьи, в настоящем виде не отражающее объективные признаки преступления, а также конкретизировать временные рамки и содержание отдельных понятий в ч. 3.

А.А. Баюш,
аспирант Университета прокуратуры
Российской Федерации

Экстерриториальность защиты прав субъектов персональных данных в рамках процесса цифровизации

Наблюдая за быстро развивающимся миром и поглощающей нас цифровой реальностью, невольно задаешься вопросом: «А защищены ли мы в новом информационном пространстве – ноосфере XXI века?»[1]. Так ли все хорошо на самом деле, или мы вступаем в новый мир, где условия выживания гораздо жестче, при этом не стоит забывать – информационная кибербезопасность в целом развита не везде, а в силу электронно-цифрового разрыва различных стран квалифицированные специалисты и дипломированные эксперты в области информационной безопасности есть не всегда. Появление огромного количества электронных средств, информационных систем в совокупности со свободным доступом к программам и информационным ресурсам привело не только к положительным, но и к отрицательным результатам – неукоснительному росту так называемых компьютерных преступлений (преступлений в сфере IT, киберпреступлений), ответственность за совершение которых регламентирована законодателем в гл. 28 УК РФ и которым зачастую сопутствует неправомерное использование и распространение персональных данных (далее – ПДн) физических лиц, их личной информации.

Так, согласно данным Генеральной прокуратуры Российской Федерации[2], только за 2020 г. количество преступлений, совершенных в сфере IT (компьютерной информации), превысило показатель прошлых лет в три раза (в 2018 г. – 174 674, в 2020 г. – 510 396). Также согласно данным МВД России о состоянии преступности за январь – декабрь 2020 г.[3], общее количество преступлений в сфере компьютерной информации возросло на 73,4%, что говорит об актуальности защиты прав субъектов ПДн.

---

[1] Как информационного этапа ноосферогенеза (формирование и развитие ноосферы).

[2] Состояние преступности в России за январь – ноябрь 2020 года: стат. сб. / Ген. прокуратура Рос. Федерации, Главное управление правовой статистики и информационных технологий. М., 2020. С. 6.

[3] Состояние преступности в России за январь – декабрь 2020 года: стат. сб. / МВД России. М., 2020. С. 31.

В первую очередь защита личной информации лежит на нас самих (учет целесообразности указания личных сведений), во-вторых, ответственность как за надлежащую обработку ПДн, так и за их неправомерное использование и распространение будет лежать на тех, кто хранит, обрабатывает и предоставляет доступ к таким данным, т.е. на операторах – лицах, к которым относятся как физические лица, так и юридические в качестве компаний, групп предприятий и организаций, а также органы государственной власти, агентства, службы и их представители.

Следует отметить, что наиболее важными нормативными правовыми актами в вопросе защиты ПДн представляются в первую очередь международные декларации и конвенции (договоры и соглашения). Так, законодатель Российской Федерации в области защиты прав субъектов ПДн ориентируется на основные положения следующих международных актов:

Окинавской хартии глобального информационного общества[1];

Конвенции ETS № 108[2] (с учетом поправок и подписанного Россией Протокола) (далее – ETS № 108), цель которой – защита прав физических лиц при осуществлении операторами автоматизированной обработки их ПДн;

Регламента ЕС № 2016/679[3] (далее – GDPR), направленного на защиту прав физических лиц при обработке ПДн последних в целом и регулирующего правила обращения обрабатываемых ПДн;

Методических рекомендаций DPIA[4], представленных в виде руководства по предусмотренной GDPR оценке различного рода

---

[1] Окинавская хартия глобального информационного общества: принята на о. Окинава 22.07.2000, договаривающиеся стороны: Великобритания, Германия (ФРГ), Италия, Канада, Россия, США, Франция, Япония // Дипломат. вестн. 2000. № 8.

[2] Конвенция о защите физических лиц при автоматизированной обработке персональных данных (ETS № 108) [рус., англ.]: заключена в г. Страсбурге 28.01.1981 // СЗ РФ. 2014. № 5. С. 419.

[3] Регламент № 2016/679 Европейского парламента и Совета Европейского союза «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС» (Общий Регламент о защите персональных данных) [рус., англ.]: принят в г. Брюсселе 27.04.2016 // Official Journal of the European Union, 04.05.2016. URL: http://eur-lex.europa.eu/ (дата обращения: 23.01.2021).

[4] DPIA: Data Protection Impact Assessments under the GDPR – a guide. // I-SCOOP. 10. 2017.

воздействия на ПДн (т.е. аудит их защищенности, проведение контрольно-надзорных мероприятий) и т.д.

Ратификация международных соглашений и имплементация норм международного права в российское законодательство в значительной мере способствуют не только укреплению положения государства на международной арене (появлению дополнительных гарантий к соглашениям), но и прогрессивному правотворчеству с учетом международной практики в реалиях сложившейся российской правовой системы в целях соответствия международным и общеевропейским принципам и стандартам. Данную тенденцию можно проследить как в Федеральном законе от 27.07.2006 № 149 «Об информации, информационных технологиях и о защите информации», в котором внимание уделяется трактованию понятия информации[1], конфиденциальности, распространения и доступа к последней, информационным системам и др., так и в Указе Президента Российской Федерации от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы», где упоминаются такие актуальные направления, как обработка больших объемов данных, интернет вещей, облачные вычислительные сервисы и др. Более того, деятельность по защите прав субъектов ПДн в России возложена на надзорный орган в лице Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

В Конвенции ETS № 108 главной целью представляется не столько защита личных сведений лица, сколько защита основных прав и свобод физического лица при осуществлении автоматизированной обработки таких данных, иначе говоря, при парсинге, реализующемся при обработке «сырых данных» (big data)[2]. Она была заключена еще в 1981 г., а в России вступила в силу только с 1 сентября 2013 г. Данный международный акт положил начало системе санкций в национальном законодательстве в сфере защиты ПДн, а именно способствовал появлению Федерального

---

[1] К ней приравниваются данные, сведения и сообщения.

[2] *Рожкова М.А.* Разрешение вопроса о легальности парсинга (скрапинга) в деле ВКонтакте v. Double Data // Комментарий практики рассмотрения арбитражных споров (судебно-арбитражной практики). Вып. 27 / под ред. В.М. Жуйкова. М.: ИЗиСП при Правительстве РФ; Юрид. фирма «КОНТРАКТ», 2020.

закона от 27.07.2006 № 152-ФЗ «О персональных данных», что оговаривается в ст. 10 ETS № 108, посвященной системе санкций за нарушение установленных требований в рамках национального законодательства в данной области.

GDPR – регламент с жесткими требованиями, невыполнение которых может повлечь за собой не только наложение крупного денежного административного штрафа (до 20 млн евро или около 4% от общего годового дохода), но и ограничение на обработку ПДн вплоть до полного запрета на осуществление такой деятельности. Данный акт – это сильно видоизмененная версия отмененной в 2018 г. Директивы о защите лиц при обработке ПДн (Директива № 95/46/ЕС). В рамках GDPR рассматриваются данные, относящиеся к ПДн идентифицируемого субъекта, это могут быть различного рода сведения об устанавливаемом субъекте ПДн, позволяющие напрямую либо косвенно установить данное лицо с помощью так называемых особых идентификаторов в виде Ф.И.О., включая удостоверяющие его документы, фактическое местоположение лица (его геолокация, история перемещений, трекинг и др.), активность пользователя в сети «Интернет» (цифровые следы в виде процессов авторизации, модель поведения в виде аккаунтинга и т.д.), сведения о доходах (декларации о доходах в налоговых органах) и здоровье (генетические и биометрические данные) и т.п. В то время как под обработкой[1] понимается любая операция с ПДн устанавливаемого субъекта как с применением автоматизированных систем, так и без использования последних, которые в целом должны обеспечивать защиту от вмешательства (конфиденциальность) и целостность ПДн, а также оперативную самовосстанавливаемость (устойчивость) таких систем при технических сбоях и неполадок иного характера в целях получения доступа к ПДн.

Также одно из главных преимуществ GDPR – так называемая защита ПДн «по умолчанию», выражающаяся не только в об-

[1] Пункт 2 ст. 4 GDPR: «...любая операция или набор операций, осуществляемых с персональными данными, с применением автоматизированных средств или без таковых, например, сбор, запись, организация, структурирование, хранение, модификация и изменение, извлечение, консультирование, использование, раскрытие посредством передачи, распространение или предоставление иным способом, упорядочение или комбинирование, ограничение, стирание или разрушение».

работке, но и в обезличивании и псевдонимизации (особый вид обезличивания), современной криптографической защите с возможностями использования различных ключей шифрования, электронной подписью и др. Под действие данного акта стал попадать и российский рынок товаров и услуг (например, Аэрофлот, РЖД, сети отелей и др.), представители которого осуществляют обработку ПДн граждан и резидентов ЕС не на территории последней, именно в этом заключается его принцип экстерриториального действия (расширенный территориальный принцип действия). GDPR осуществляет не только контроль трансграничной обработки ПДн, но и «процедуру регулярной проверки и оценки эффективности технических и организационных мер для обеспечения безопасности обработки» (п. d ст. 32 GDPR). Так, был расширен перечень споров, которые не могут быть рассмотрены комиссией государственного органа по служебным спорам. Данный список был дополнен пунктом о неправомерных действиях нанимателя (руководитель государственного органа или государственное должностное лицо) по обработке ПДн, а также по защите ПДн служащего, такие споры должны передаваться в суд[1].

Данный регламент существенно влияет и на российскую правовую реальность, а именно на процесс прохождения аудита по оценке защищенности ПДн, что повлекло как внедрение нового программного обеспечения, так и принятие новых правил обработки ПДн и преобразование соответствующей политики конфиденциальности, что в совокупности позволяет уменьшить, а иногда и предотвратить случаи утечки, ошибки в сборе и обработке личной информации физических лиц. Более того, положения GDPR о правах на забвение субъекта ПДн, на перенос ПДн, на оповещение об их утечке и нарушении обработки, а также отдельные положения об особой защите ПДн несовершеннолетних лиц (детей) и иные могут быть хорошим подспорьем для дальнейшего совершенствования российского законодательства в данной области.

[1] Федеральный закон от 20.07.2020 № 227-ФЗ «О внесении изменений в статью 70 Федерального закона «О государственной гражданской службе Российской Федерации».

Т.М. Петрова,
аспирант Санкт-Петербургского
юридического института (филиала)
Университета прокуратуры
Российской Федерации

Уголовная ответственность за незаконные приобретение или продажу особо ценных диких животных, занесенных в Красную книгу, с использованием сети «Интернет»

За последние 40 лет на нашей планете исчезло около половины редких видов диких животных и растений. Основные причины – это изменение климата, утрата мест обитания, браконьерство и незаконная торговля[1]. Определяющим фактором масштабного истребления таких биоресурсов считается высокий спрос на особи и их производные как на международном рынке, так и на территории нашей страны. Незаконный оборот животных, находящихся под угрозой исчезновения, уже давно считается одним из наиболее прибыльных видов нелегального бизнеса.

В Российской Федерации в соответствии с новым Перечнем объектов животного мира, занесенных в Красную книгу, к вероятно исчезнувшим и находящимся под угрозой исчезновения относятся 33 вида птиц, 35 видов млекопитающих, 21 вид рыб[2].

Уголовное законодательство с 2013 г. предусматривает ответственность за незаконные добычу и оборот особо ценных диких животных и водных биологических ресурсов, принадлежащих к видам, занесенным в Красную книгу Российской Федерации и (или) охраняемым международными договорами Российской Федерации. В Уголовный кодекс Российской Федерации введена ст. 258[1]. Закрепленная в ней уголовно-правовая норма характеризуется непростым строением и охватывает два самостоятельных состава. Перечень особо ценных видов диких животных и водных биологических ресурсов утвержден постановлением

[1]URL: https://www.belta.by/world/view/v-mire-za-40-let-ischezlo-okolo-poloviny-redkih-vidov-dikih-zhivotnyh-i-rastenij-236184-2017/ (дата обращения: 07.01.2021).
[2] URL: http://publication.pravo.gov.ru/Document/View/0001202004020020?index=9&rangeSize=1 (дата обращения: 25.01.2021).

Правительства Российской Федерации от 31.10.2013 № 978[1], который к таковым относит 22 вида млекопитающих, рыб и птиц.

В 2018 г. статья дополнена ч. 1[1], предусматривающей ответственность за незаконные действия в виде приобретения и продажи указанных биоресурсов с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей, в том числе сети «Интернет». Внесение в закон дополнений предопределено глобальным значением телекоммуникационной сети «Интернет» в последние годы практически во всех сферах жизни общества. Через данную сеть реализуется преступный умысел лиц, осуществляющих незаконную торговлю особо охраняемыми животными и растениями. С использованием таких средств связи виновные лица ведут поиск предложений о приобретении или продаже предмета преступления путем размещения соответствующих объявлений, договариваются о способах и видах оплаты по сделке, передаче предмета сделки.

Одним из способов препятствования незаконной торговле исчезающими видами животных является мониторинг соответствующей информации в сети «Интернет». Органами прокуратуры Российской Федерации систематически осуществляется данная работа и при нахождении ресурсов, содержащих запрещенные сведения, в суды направляются исковые заявления о признании информации, распространенной посредством сети «Интернет», запрещенной на территории Российской Федерации. Согласно ч. 6 ст. 10 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» запрещается распространение информации, за которую предусмотрена административная или уголовная ответственность.

Так, в ноябре 2020 г. в Костромской области прокуратурой пресечена продажа бивней и рогов «краснокнижного» нарвала[2].

---

[1] Постановление Правительства РФ от 31.10.2013 № 978 «Об утверждении перечня особо ценных диких животных и водных биологических ресурсов, принадлежащих к видам, занесенным в Красную книгу Российской Федерации и (или) охраняемым международными договорами Российской Федерации, для целей статей 226[1] и 258[1] Уголовного кодекса Российской Федерации».

[2] URL: https://www.interfax-russia.ru/center/news/kostromskaya-prokuratura-dobilas-blokirovki-saytov-po-prodazhe-chastey-zhivotnyh-zanesennyh-v-krasnuyu-knigu (дата обращения: 25.01.2021).

В Липецкой области работники прокуратуры обратились в суд с иском о признании незаконными интернет-ресурсов о продаже болотных черепах, занесенных в Красную книгу РФ[1]. По решению суда подобные сайты вносятся в Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено[2]. После внесения ресурсов в реестр доступ к ним ограничивается.

Совершая незаконную покупку особо ценных видов диких животных, их частей и дериватов с использованием сети «Интернет», лицо становится субъектом преступления, предусмотренного ч. 1^1 ст. 258^1 УК РФ. Наиболее распространенным проявлением данного состава является приобретение икры осетрового вида, которая не имеет соответствующей маркировки на таре. Такое деяние квалифицируется как незаконное приобретение имущества, заведомо добытого преступным путем. Ответственность за совершение такой сделки при этом несет не только продавец осетровой икры, но и покупатель, осознающий общественную опасность совершаемого деяния. Также предметом незаконной покупки могут быть части редких диких животных – рога сайгака, клыки снежного барса, кости амурского тигра, шкуры и дериваты-чучела животных, которые для субъекта, как правило, являются элементами коллекций[3].

При квалификации деяний, совершенных посредством сети «Интернет» либо иных информационных ресурсов, когда они совершаются путем приобретения либо продажи предмета преступ-

---

1

URL: https://chr.aif.ru/lip/events/v_lipeckoy_oblasti_presekli_prodazhu_krasnoknizhnoy_bolotnoy_cherepahi (дата обращения: 25.01.2021).

2 Приказ Роскомнадзора от 03.08.2017 № 152 «Об утверждении порядка взаимодействия оператора единой автоматизированной информационной системы «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено» с уполномоченными органами и правоохранительными органами».

3 *Скворцова О.В., Шарапа Р.А.* Уголовная ответственность за незаконный оборот особо ценных диких животных, занесенных в Красную книгу, с использованием сети «Интернет» // Уч. зап. Крым. федер. ун-та им. В.И. Вернадского. Юрид. науки. 2019. Т. 5 (71). № 1. С. 187.

ления, на практике могут возникнуть трудности с применением нужной уголовно-правовой нормы. Рассматриваемая статья 258^1 УК РФ содержит ч. 2, п. «б» которой устанавливает уголовную ответственность за незаконные добычу и оборот особо ценных видов биоресурсов с публичной демонстрацией, в том числе в средствах массовой информации или информационно-телекоммуникационных сетях, включая сеть «Интернет». В научной литературе высказывается следующая позиция о соотношении между собой ч. 1^1, а также ч. 2^1 и 3^1 и п. «б» ч. 2 ст. 258^1 УК РФ. Преступное деяние квалифицируется по ч. 1^1, 2^1 и 3^1 ст. 258^1 УК РФ в случаях, если средства массовой информации либо электронные или информационно-телекоммуникационные сети, в том числе сеть «Интернет», используются для обеспечения совершения общественно опасного деяния. К примеру, с их помощью достигается соглашение о совершении сделки, посредством электронных средств осуществляются платежи, размещается реклама в средствах массовой информации или в информационно-телекоммуникационных сетях, в том числе в сети «Интернет». Если же посредством средств массовой информации или информационно-телекоммуникационных сетей, включая сеть «Интернет», публично демонстрируется процесс или результат приобретения или продажи предмета преступления, предусмотренного ст. 258^1 УК РФ, содеянное следует квалифицировать по п. «б» ч. 2 или по ч. 3 ст. 258^1 УК РФ[1].

Положения об уголовной ответственности за незаконные приобретение и продажу с помощью сети «Интернет» распространяются лишь на особо ценные виды диких животных, к которым отнесено 22 вида. В отношении иных редких и исчезающих животных такой ответственности не предусмотрено. При совершении таких преступлений возникают сложности и с определением видовой принадлежности животного, так как в объявлениях, размещенных в сети, подобная информация преступными лицами намерено скрывается.

Таким образом, проблема защиты особо ценных видов диких животных уголовно-правовыми мерами многогранна и имеет

---

[1] *Малыхина Т.А.* Уголовно-правовое значение признаков объективной стороны преступлений, предусмотренных статьей 258^1 Уголовного кодекса Российской Федерации // Юрид. наука и правоохран. практика. 2019. № 2 (48). С. 58–59.

множество аспектов как теоретического, так и практического характера, требующих научного осмысления и изучения. Многие вопросы законодательной регламентации уголовно-правовых норм, устанавливающих ответственность за преступления против особо ценных диких животных, а также дифференциация ответственности по ним требуют разрешения в целях дальнейшего совершенствования и развития.

С.В. Мурадян,
старший преподаватель кафедры
Московского университета
МВД России имени В.Я. Кикотя,
кандидат юридических наук

Д.М. Кулиджанян,
курсант Московского
университета МВД России
имени В.Я. Кикотя

Особенности квалификации преступлений, совершенных с использованием информационно-коммуникационных технологий и в сфере компьютерной информации

Компьютерная информация стала неотъемлемым элементом функционирования всех отраслей экономики, социальной сферы, сферы обеспечения жизнедеятельности общества, обороны любого государства и т.п. Любые новые технологии – это всегда несовершенство законодательной системы, призванной регулировать общественные отношения в данной области. А имеющиеся пробелы – привлекательные способы осуществления противоправных действий.

Рассматривая нормативное регулирование преступлений, совершенных с использованием цифровых технологий, следует отметить, что такие понятия, как «преступления в сфере компьютерной информации» и «преступления, совершенные с использованием информационно-коммуникационных технологий», не схожи между собой по смысловому составу. Исходя из этого в

данной статье мы рассматривали преступления в сфере компьютерной информации как составную часть преступлений, совершенных с использованием компьютерных технологий. С использованием информационно-коммуникационных технологий можно совершить большое количество преступлений, содержащихся в различных статьях Особенной части Уголовного кодекса Российской Федерации. Такой способ лишь облегчает возможность посягательства на основной объект преступления.

В связи с ограниченным объемом работы особое внимание мы уделим преступлениям, совершаемым в сфере компьютерной информации.

Общественная опасность таких преступлений состоит в том, что неправомерное изменение данных в информационной системе может повлечь за собой тяжкие последствия, угрожающие жизни и здоровью граждан, работе средств связи и транспорта, нормальному функционированию энергетики и гидроэнергетики, а также других сфер общественной жизни.

Нормативное регулирование анализируемых деяний реализуется путем закрепления в гл. 28 УК РФ следующих составов преступлений: ст. 272 (Неправомерный доступ к компьютерной информации); ст. 273 (Создание, использование и распространение вредоносных компьютерных программ); ст. 274 (Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей); ст. 274^1 (Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации).

Сущность данных составов заключается в недопущении наступления общественно опасных последствий путем совершения преступлений с использованием компьютерных технологий, при этом компьютер будет являться средством совершения преступления.

Родовым объектом данных преступлений выступают общественные отношения, связанные с охраной общественного порядка и общественной безопасности. Видовым объектом будут являться общественные отношения в сфере обеспечения безопасности компьютерной информации. Среди прочих видов безопасности информационная безопасность является одним из самых неопределенных видов безопасности, так как с развитием техноло-

гий растет разновидность и сложность компьютерных носителей, вследствие чего информационная безопасность становится все более многогранным и сложным видом безопасности.

Непосредственный объект преступлений, предусмотренных статьями гл. 28 УК РФ, определяется исходя из названия статей. Между тем указанные преступления могут затрагивать и иные стороны общественной жизни, в связи с чем можно говорить о наличии дополнительного объекта преступления, например, тайна личной переписки (дополнительный объект – общественные отношения, обеспечивающие личные права человека), данные, составляющие государственную (дополнительный объект – общественные отношения, обеспечивающие безопасность государства в части, касающейся государственной тайны) и иные виды тайны, и пр.

Предметом преступлений, предусмотренных гл. 28 УК РФ, будет являться компьютерная информация. Определение компьютерной информации следует искать в примечании 1 к ст. 272 УК РФ.

Объективная сторона составов преступлений, предусмотренных гл. 28 УК РФ, выражается как в действиях, так и в бездействии. Причем бездействие возможно только в рамках реализации объективной стороны ст. 274 и ч. 3 ст. 274[1] УК РФ. В случае материальных составов преступлений (ст. 272, 274 и ч. 3 ст. 274[1]) действие либо бездействие должно повлечь за собой общественно опасные последствия. Правоприменителям предстоит также доказывать причинно-следственную связь между ними. В рамках формальных составов преступлений необходимо только установить факт действия.

Интересными являются случаи, когда имеющиеся технические средства позволяют восстановить утраченную в порядке ст. 272 УК РФ информацию. Получается, что преступление было окончено исполнителем и наступил результат, ожидаемый субъектом преступления. Однако результат был изменен потерпевшим по не зависящим от лица обстоятельствам. В данном случае следует говорить о покушении на уничтожение охраняемой законом компьютерной информации (ч. 1 ст. 272 и ч. 3 ст. 30 УК РФ)[1].

---

[1] *Русскевич Е.А.* Уголовное право и «цифровая преступность»: проблемы и решения: монография. М., 2019. С. 145.

Временем совершения преступления следует считать момент нажатия клавиши компьютера, запускающей конечную команду. В данном случае не имеет значения, когда наступили последствия и с какого информационного носителя была произведена команда. Временной интервал может составлять от нескольких недель до считанных секунд. Это связано с объемом внедряемой вредоносной программы, функционированием технологии, с которой совершается преступление, и т.д.

Если со временем все относительно просто, то с местом совершения преступления возникает ряд проблем. Неоспоримым фактором привлекательности сферы применения компьютерной информации является мнимая видимость «недосягаемости» субъекта преступления, поскольку преступление совершается в одном месте, а последствия происходят в другом.

Местом совершения преступления может быть как место совершения деяния, место окончания деяния, так и место наступления общественно опасных последствий. Львиная доля преступлений, совершенных с использованием компьютерных технологий, происходит в сетях, это значит, что зачастую средства совершения преступлений и общественно опасные последствия расположены в разных местах. Ответ на вопрос о месте совершения преступления каждый раз решается индивидуально. Например, в случае заявления потерпевшего в территориальный орган местом преступления будет являться место обращения потерпевшего в полицию.

Говоря о месте совершения компьютерных преступлений, следует отметить правомочность государства в расследовании данных преступлений. Здесь речь идет о том, что субъект преступления совершил преступление в одном государстве, а общественно опасные последствия произошли в другом. В случае если это произошло на территории Содружества Независимых Государств, то данный вопрос будет регулироваться в соответствии с Конвенцией о правовой помощи и правовых отношениях по гражданским, семейным и уголовным делам, заключенной в Минске 22 января 1993 г. В соответствии с данной Конвенцией страны, входящие в Содружество Независимых Государств, могут объединиться в целях расследования преступлений, совершенных с использованием компьютерных технологий. В случае с

другими государствами, не входящими в состав СНГ, вопрос о месте совершения преступления, а также где оно будет расследоваться, будет решаться на основании договоренности между сторонами. В Российской Федерации для таких мероприятий существует специальное подразделение МВД России Управление «К».

Наглядным примером может служить дело В. Левина, который с помощью компьютера, находящегося в офисе фирмы в Санкт-Петербурге, вводил ложные данные в систему Ситибанка, расположенного в США, в результате чего со счетов вкладчиков было похищено более 10 млн долл. В. Левин скрывался от следствия, был задержан и осужден в Лондоне. При этом Великобритания отказала в выдаче преступника США и России, мотивируя это тем, что законодательство страны не регламентирует ситуацию, когда преступление совершено на территории одного государства, а последствия наступили на территории другого.

Проблема определения места совершения преступления остро стоит не только на межгосударственном, но и на межрегиональном уровне. В пределах последнего материалы уголовного дела направляются на место окончания преступления, вследствие чего затягиваются сроки раскрытия преступления, а также происходит утеря информационных следов преступления.

Субъектом преступлений, предусмотренных ст. 272, 273 274 УК РФ, является вменяемое физическое лицо, достигшее возраста 16 лет. По ст. 274^1 УК РФ субъектом преступления признается лицо, на которое возложена ответственность за соблюдение правил по эксплуатации соответствующих сетей связи. Фактически ст. 274^1 является специальной по отношению к остальным статьям гл. 28 УК РФ. Следовательно, специальный субъект предусмотрен только в этом составе преступления. По остальным статьям гл. 28 УК РФ субъект преступления общий.

Субъективная сторона рассматриваемых деяний может характеризоваться как умышленной, так и неосторожной формой вины. Среди мотивов, характерных для всех компьютерных преступлений, преобладают два основных: корысть и «интеллектуальный вызов», т.е. стремление продемонстрировать собственный профессионализм.

Общим моментом, объединяющим все преступления информационного характера, является использование в конструк-

ции их составов терминов, обозначающих различные информационные явления. Указанные термины должны употребляться, во-первых, корректно, с точки зрения теории информации, а во-вторых, единообразно во всем тексте уголовного закона. Нарушение этих требований будет означать несоблюдение таких принципов криминализации, как беспробельность закона и неизбыточность запрета, а также определенность и единство терминологии.

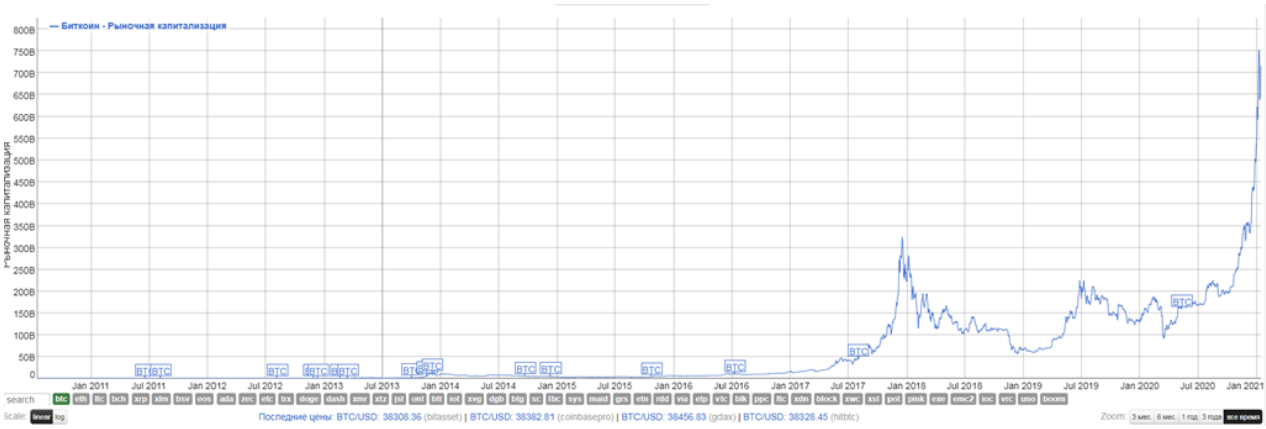
Подводя итог сказанному, можно сделать вывод, что специфика гл. 28 УК РФ состоит в том, что она содержит преступления, раскрытие и расследование которых требует специальных знаний и навыков со стороны правоприменителей, а также использования дополнительного дорогостоящего оборудования и программного обеспечения. Такие преступления совершаются образованными людьми с высоким уровнем интеллекта путем использования «интеллектуальных средств» и орудий преступления. В ответ на существующие тенденции в Московском университете МВД России им. В.Я. Кикотя на факультете информационной безопасности готовят сотрудников полиции по борьбе с указанными видами преступлений. Аналогичные факультеты и направления в учебе существуют в большинстве вузов правоохранительных органов России.

М.Г. Терехов,
соискатель кафедры гражданского
и трудового права, гражданского
процесса Московского университета
МВД России имени В.Я. Кикотя,
инспектор отдела международного
сотрудничества Московского
университета МВД России
имени В.Я. Кикотя

Межотраслевой институт цифровых активов: типологии криптовалют

В настоящее время особое внимание пользователей различных стран (с разным развитием экономической составляющей страны – ВВП) в глобальной сети «Интернет» ориентировано на цифровые правоотношения, цифровые технологии в области экономики, которые основаны на принципах децентрализации, низкой комиссии при транзакциях, безопасности цифровых активов.

Распространенным финансовым инструментом цифровых правоотношений являются цифровые активы. В 2017 г. пик капитализации криптовалютного рынка достиг рекордных 109 614 236 754 млрд долл. только в одну разновидность криптовалют – биткоины при рыночном курсе цены биткоина на криптовалютных биржах в размере 6576 долл. за 1 биткоин. По состоянию на январь 2021 г. рыночная стоимость 1 биткоина составляет 38 388,96 долл., что обусловливает уверенную тенденцию развития криптовалют.



Курс капитализации биткоина

В различных своих видовых проявлениях родоначальником цифровых активов служит криптовалюта биткоин «народные деньги» из-за децентрализации и отсутствия возможности контроля органами власти.

Период с 2018 по 2019 г. стал тяжелым для сферы цифровых активов. Активный спад криптовалютных курсов по всем позициям на первое полугодие 2019 г. необъясним. Постоянная волатильность криптовалют из-за непредсказуемости и неизученности с точки зрения классических экономических теорий, которые стали неэффективны при применении к цифровым активам, является фактором, побуждающим более подробно изучать сформировавшуюся проблематику с точки зрения экономических и юридических наук.

Проблема, с которой столкнулась цифровая экономика, обусловливает появление более совершенных типологий криптовалют, которые отвечают вызовам современности в цифровых правоотношениях, связанных с оборотом цифровых активов[1].

Новым цифровым активом, замещающим перспективу классических криптовалют, становится в настоящее время стейблкоин, который значительно изменил свою политику относительно классических криптовалют. Основополагающая идея стейблкоина – гибридность криптовалют. Данный цифровой актив в отличие от классической криптовалюты обеспечивается различного рода ценным имуществом: таким может выступать золото в соотношении 1 к 1, т.е. 1 монета стейблкоина равна 1 г золотого актива. Из практической информации следует, что ценные активы охраняются определенной компанией (маркой, под которой выступает тот или иной стейблкоин) в материальном мире, а также другие ценности, в частности фиатные деньги. Родоначальником стейблкоинов выступает монета Tether.

---

[1] *Тумаков А.В., Терехов М.Г.* Создание финансовых пирамид с использованием цифровых активов // Вестн. экон. безопасности. 2020. № 3. URL: https://cyberleninka.ru/article/n/sozdanie-finansovyh-piramid-s-ispolzovaniem-tsifrovyh-aktivov (дата обращения: 10.11.2020).

2. Tether (19,43%)

#	Source	Pair	Volume (24h)	Price	Volume (%)
1	Binance	BTC/USDT	$379 383 000	$1,00	10,55%
2	OKEx	BTC/USDT	$185 759 000	$1,00	5,16%
3	Huobi	EOS/USDT	$157 606 000	$1,00	4,38%
4	Huobi	BTC/USDT	$134 176 000	$1,00	3,73%
5	OKEx	EOS/USDT	$118 659 000	$1,00	3,30%
6	Binance	EOS/USDT	$114 934 000	$1,00	3,20%
7	ZB.COM	DASH/USDT	$105 548 000	$0,998700	2,93%
8	Binance	ETH/USDT	$99 436 900	$1,01	2,76%
9	OKEx	ETH/USDT	$90 036 400	$1,01	2,50%
10	ZB.COM	BTC/USDT	$82 644 200	$1,00	2,30%
		View More			
Total/Avg			**$3 597 212 799**	**$1,00**	

Таблица основного объема капитализации, курса, предполагаемого роста курса «золотой десятки стейблкоинов»

Растущая популярность стейблкоинов объясняется, как уже отмечалось, волатильностью курсов криптовалют на криптовалютных биржах[1].

Криптовалюты переводят в стейблкоины во избежание рисков, присутствующих с плавающим курсом той или иной криптовалюты, а также для сохранения актуальности своих цифровых криптовалютных активов и возможности их натурализации без финансовых потерь.

Все модернизирующееся в области первоначальных классических криптовалют[2] можно назвать своеобразной эволюцией, которая несет в себе (как в финансовом инструменте) с каждым разом все больше новых предложений по развитию, упрощению оборота цифровых активов на просторах сети «Интернет». По-

[1] *Andreas M.* Antonopoulos, Mastering Bitcoin: Unlocking Digital Crypto currencies, 2016. P. 298.

[2] Федеральный закон от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации».

добные естественно складывающиеся модернизации в области цифровых активов следует определить как государственную необходимость правового регулирования такого рода правоотношений, связанных с разграничением свойств и особенностей цифровых активов.

Через призму государственной программы «Цифровая экономика Российской Федерации» проблематика возникновения и использования в сети «Интернет» цифровых активов (типовое ответвление – стейблкоин), определяется в данной статье как взаимосвязанный финансовый элемент института цифровых активов, который законодательно не урегулирован в России, а также затрагивает два из трех уровней развития цифровой экономики:

1. Платформы и технологии, где формируются компетенции для развития рынков и отраслей экономики (сфер деятельности)[1].

2. Среда, которая создает условия для развития платформ и технологий и эффективного взаимодействия субъектов рынков и отраслей экономики (сфер деятельности) и охватывает нормативное регулирование, информационную инфраструктуру, кадры и информационную безопасность.

Так, Концепция развития гражданского законодательства Российской Федерации (одобрена Советом при Президенте Российской Федерации по кодификации и совершенствованию гражданского законодательства 7 октября 2009 г.) определяет многогранность правовых отношений, образуемых в области гражданского законодательства, также указывая на обширность практики и необходимость ее совершенствования в гражданском законодательстве. Совокупность изложенных и обоснованных научных доводов позволяет выступить с научной аксиомой о существовании именно типологий криптовалют (цифровых активов), которые могут быть разделены по типу – обеспеченности, что поможет в дальнейшем более точно исследовать проблематику оборота цифровых активов как в юридических, так и в экономических науках.

---

[1] *Kirk D.P.* The Ultimate Bitcoin Business Guide: For Entrepreneurs & Business Advisors, 2015. P. 330.

М.А. Синолиц,
студент Юридического института
Российского университета
транспорта (МИИТ)

Уголовная ответственность за распространение ложной информации в сети «Интернет» о пандемии коронавирусной инфекции

Год назад мир столкнулся с новой болезнью – COVID-19. С английского аббревиатура расшифровывается как COronaVIrus Disease[1]. Россию этот недуг также не обошел стороной. Постановлением Правительства Российской Федерации коронавирусную инфекцию внесли в перечень заболеваний, представляющих опасность для окружающих[2].

Люди, столкнувшись с неизвестным заболеванием, начали обращаться к всевозможной доступной информации. В современном обществе сведения распространяется разными путями. Один из востребованных способов среди населения нашей страны – это использование сайтов сети «Интернет». Любые публикуемые данные должны соответствовать принципам правового регулирования отношений, возникающих в сфере информации, информационных технологий и защиты информации, – информация должна быть достоверной и предоставляться своевременно. Также в законе закреплен принцип о свободе поиска, получения, передачи, производства и распространения информации любым законным способом[3]. Однако доверчивый пользователь попадает в ловушку недостоверной (фейковой) информации перенасыщеного информационного пространства сети «Интернет». Фейк – в данном случае упрощенное название недостоверной информации. Эта информация никого не оскорбляет, но угрожает жизни и

[1] Сайт Всемирной организации здравоохранения. Европейское региональное бюро. URL: https://www.euro.who.int/en/health-topics/health-emergencies/novel-coronavirus-2019-ncov_old (дата обращения: 10.02.2021).
[2] Постановление Правительства РФ от 31.01.2020 № 66 «О внесении изменения в перечень заболеваний, представляющих опасность для окружающих».
[3] Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

имуществу, общественной безопасности или работе важной инфраструктуры.

Ложные сообщения о пандемии, размещаемые на интернет-ресурсах, подрывали борьбу с распространением коронавирусной инфекции, сеяли панику, вводили в заблуждение о результатах разработки и применении вакцины и др. Ответом стало ужесточение ответственности и введение новых статей в УК РФ. Наказание за публичное распространение ложной информации с 1 апреля 2020 г. предусматривается ст. 207^1 и 207^2 УК РФ[1].

В данных статьях объектом преступления выступает общественная безопасность, предметом преступления считается заведомо ложная информация, угрожающая общественной безопасности. Верховный Суд Российской Федерации уточняет, что для наступления уголовной ответственности информация должна быть заведомо ложной и изначально не соответствовать действительности, о чем достоверно было известно лицу, ее распространявшему. Такое общественно опасное деяние и будет объективной стороной преступления. Для правильного понимания и правоприменения рассматриваемых статей нужно учитывать содержание бланкетных норм, специальных терминов и государственных стандартов. Для применения ст. 207^2 УК РФ необходимо выполнение условия наступления последствий в виде причинения вреда здоровью человека или его смерти или иных тяжких последствий, также должна прослеживаться причинно-следственная связь между преступными последствиями и распространенными заведомо ложными сведениями.

Статья 207^1 УК РФ предусматривает наказание в виде штрафа в размере от 300 тыс. до 700 тыс. руб. или в размере заработной платы или иного дохода осужденного за период от одного года до 18 месяцев, либо обязательных работ на срок до 360 часов, либо исправительных работ на срок до одного года, либо ограничения свободы на срок до трех лет.

Статья 207^2 УК РФ предусматривает наказание в виде штрафа в размере от 700 тыс. до 1,5 млн руб. или в размере заработной платы или иного дохода осужденного за период до 18 ме-

[1] Федеральный закон от 01.04.2020 № 100-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статьи 31 и 151 Уголовно-процессуального кодекса Российской Федерации».

сяцев, либо исправительных работ на срок до одного года, либо принудительных работ на срок до трех лет, либо лишения свободы на тот же срок (ч. 1); в виде штрафа в размере от 1,5 млн до 2 млн руб. или в размере заработной платы или иного дохода осужденного за период от 18 месяцев до трех лет, либо исправительных работ на срок до двух лет, либо принудительных работ на срок до пяти лет, либо лишения свободы на тот же срок (ч. 2).

Размещение лицом в сети «Интернет» или иной информационно-телекоммуникационной сети, в частности на своей странице или на странице других пользователей, материала, содержащего ложную информацию (например, видео-, аудио-, графического или текстового), созданного им самим или другим лицом (в том числе так называемый репост), может быть квалифицировано по ст. 207^1 или 207^2 УК РФ только в случаях, когда установлено, что лицо действовало с прямым умыслом, сознавало, что размещенная им под видом достоверной информация является ложной, и имело цель довести эту информацию до сведения других лиц. Например, в Ханты-Мансийске гражданин Ф. разместил на своей странице в социальной сети Instagram с открытым (публичным) доступом неограниченного круга пользователей информационно-телекоммуникационной сети «Интернет» видеоролик с целью провокации паники среди населения и нарушения правопорядка под видом достоверного сообщения, лично записал заведомо ложные сведения о несуществовании коронавирусной инфекции (COVID-19), о недостоверности российской тест-системы по выявлению коронавирусной инфекции и призвал население к пренебрежению правилами и средствами индивидуальной защиты, установленными государственными органами. Его деяния суд квалифицировал по ст. 207^1 УК РФ, поскольку он совершил публичное распространение под видом достоверных сообщений заведомо ложной информации об обстоятельствах, представляющих угрозу жизни и безопасности граждан, и о принимаемых мерах по обеспечению безопасности населения и территорий, приемах и способах защиты от указанных обстоятельств. Наказание назначено в виде обязательных работ на срок 200 часов[1].

[1] Приговор от 29.07.2020 № 1-74/2020 по делу № 1-74/2020. URL: https://sudact.ru/regular/doc/Rb7V6qr7PSQx/ (дата обращения: 17.02.2021).

Следует отметить, что недостоверная информация может вредить абсолютно любой сфере деятельности государства и общества. Такая информация вызывает негативные психологические эффекты групповой поляризации и опровергает сложившиеся мнения посредством информационного джерримендеринга, вводя в заблуждение. Распространять ее могут как пользователь, так и новостные боты, тролли и киборги, действие которых основывается на использовании автоматизированных алгоритмов и систем искусственного интеллекта[1]. Они с помощью метода case-study могут вызывать цепные реакции каскадного типа вирусного распространения фейковых новостей[2].

Таким образом, всемирная сеть «Интернет» охватывает многомиллионную аудиторию граждан Российской Федерации: слушателей, зрителей, читателей. В связи с этим в свете последних событий важно создать единую государственную информационную базу. Правонарушители новых статей Уголовного кодекса Российской Федерации – не всегда простые обыватели, порой это деяние – высокопродуманный план для подрыва национальной общественной безопасности государства, реализуемый сообществами, где задействуются высококлассные специалисты. В своих противоправных деяниях последние используют зачастую инновационные разработки науки и техники, из-за чего можно предложить ввести в статьи дополнительные квалифицирующие признаки, предусматривающие ужесточение наказания за преступное деяние. Для борьбы с публичным распространением заведомо ложной общественно значимой информации в сети «Интернет» важна скорость обработки поступающих данных. Человекоресурс не может справиться с таким огромным потоком разнообразных сведений. Решение видится в создании глобального информационного фильтра с непосредственно интегрированным модулем проверки с использованием искусственного интеллекта. Такой комплексный подход позволит обрабатывать

---

[1] *Нестик Т.А., Михеев Е.А.* Информационные войны с использованием систем искусственного интеллекта: анализ психологических механизмов воздействия / Ин-т психологии РАН. Организационная психология и психология труда. 2019. Т. 4. № 4.

[2] *Манойло А.В.* Цепные реакции каскадного типа в современных технологиях вирусного распространения «фейковых новостей» // Вестн. Моск. гос. обл. ун-та (электрон. журн.). 2020. № 3.

массивы входящих данных практически без временных задержек публикации важных новостей. При выявлении публикации общественно опасной заведомо ложной информации требуется безотлагательная публикация опровержения или введение специального обозначения фейковой новости при невозможности ее удаления.

Граждане Российской Федерации должны быть уверены в поступающей информации. Наше спокойствие – наша безопасность.

Секция 2.
Использование цифровых технологий в предупреждении преступности

В.Ю. Голубовский,
заведующий кафедрой
уголовно-правовых дисциплин
Российского государственного
социального университета,
доктор юридических наук,
профессор

Проблемы предупреждения киберпреступности

Особую актуальность проблемы предупреждения киберпреступности обострило использование в период пандемии цифровых технологий в целях обеспечения режима самоизоляции граждан. Применяемые технологии можно подразделить на две группы в зависимости от субъектов воздействия: технологии, обеспечивающие соблюдение режима карантина гражданами, инфицированными COVID-19 (обязательные к установке мобильные приложения, контроль геолокации мобильных устройств, отслеживание перемещений граждан и автотранспорта при помощи городских камер видеонаблюдения); технологии, обеспечивающие соблюдение режима самоизоляции гражданами, не инфицированными COVID-19 (цифровые пропуска для личных нужд и передвижения автотранспорта, ограничение использования транспортных карт, регламентация прогулок вблизи места жительства).

Названные технологии обладают рядом преимуществ в сравнении с традиционными способами контроля. Так, цифровой пропуск сложнее подделать, а автоматизированный контроль обладает более высокой степенью выявления нарушений, однако и степень риска нарушения конституционных прав граждан несоизмеримо выше. В частности, беспокойство вызывают следующие аспекты: установление ограничений конституционных прав

граждан нормативными актами органов государственной власти субъектов Российской Федерации в нарушение ч. 3 ст. 55 Конституции России, закрепляющей, что основные права граждан могут быть ограничены только федеральным законом; серьезные дополнительные трудности для старшего поколения и иных отдельных групп населения, вызванные необходимостью активного взаимодействия с интернет-ресурсами; недостаточный уровень защиты персональных данных, отмечаемый IT-специалистами; нестабильность работы мобильных приложений, повлекшая значительное количество ошибочно выписанных штрафов; несоответствие ряда технологий законодательству об охране персональных данных; несоразмерность ограничительных мер в сравнении с иными случаями ограничения свободы передвижения; возможность дальнейшего использования цифровых профилей граждан по окончании пандемии.

Для минимизации указанных рисков необходимо решить вопрос о допустимости вмешательства государства в частную жизнь граждан посредством формирования и использования их цифровых профилей. Отсутствие такого профиля не может являться причиной дискриминации граждан при предоставлении государственных услуг, банковских продуктов или при приеме на работу. Использование систем распознавания лиц для розыска опасных преступников или облегчения доступа к финансовым инструментам лиц с ограниченными возможностями следует всячески приветствовать, но при условии детальной регламентации сбора и использования персональных данных. Ответственность за неправомерные действия с персональным данными граждан должна быть соразмерна в части санкций ответственности за разглашение следственной или государственной тайны.

При этом недопустимо использование технологий цифрового контроля в целях воспитания и улучшения морального облика россиян. Применение искусственного интеллекта имеет большое значение в диагностике заболеваний, снижении аварийности на дорогах и в иных сферах, однако одновременно технологии распознавания лиц и автоматизация «социального скоринга» могут привести к углублению социальной несправедливости, росту напряженности и поляризации общества. Этические принципы и

этический аудит должны предшествовать любому внедрению подобных систем и алгоритмов.

Ущерб от киберпреступности в России по итогам 2020 г. составил 69 млрд руб. К концу 2021 г., по оценке специалистов, ущерб достигнет 90 млрд руб., т.е. предполагается рост на 30%. В 2020 г. в России было совершено около 15 млн мошеннических звонков. В 2021 г., согласно прогнозу, таких звонков будет 19 млн. Для расширения охвата мошенники будут применять автоматизированный обзвон и роботизированные виртуальные колл-центры.

Ущерб от IT-преступности постоянно растет. Если в 2020 г. в России было зарегистрировано 510,4 тыс. таких преступлений, то в нынешнем году эта цифра может вырасти до миллиона. Количество киберпреступников достигнет 25 тыс.[1]

Телефонное мошенничество приобрело огромный масштаб, который можно объяснить, во-первых, доступностью и анонимностью услуг для злоумышленников, отсутствием ответственности и надзора; во-вторых, отсталостью регулирования отрасли, высокой инертностью регулятора. Правила устарели и не регламентируют подключение операторов передачи данных к телефонной сети. Опять же нечеткая формулировка Федерального закона от 07.07.2003 № 126-ФЗ «О связи», согласно которому операторы обязаны обеспечить передачу номера абонента, инициирующего вызов.

Кроме того, не работает надзор за исполнением постановления Правительства Российской Федерации от 13.07.2004 № 350 «Об утверждении Правил распределения и использования ресурсов нумерации единой сети электросвязи Российской Федерации», по которому операторам разрешено использовать номера только из выделенной установленным порядком телефонной емкости, т.е. операторы сетей не следят, а надзор не реагирует. Каждому оператору выделяется номерная емкость, которую оператор распределяет по своим абонентам в момент заключения договоров. Поэтому ситуация, когда клиент одного оператора ини-

[1] *Берегитесь* телефона. URL: https://rg.ru/2021/02/14/kak-protivostoiat-kiberprestupnosti.html (дата обращения: 21.01.2021).

циирует звонки через IP-телефонию, подставляя номер, принадлежащий другому оператору, недопустима.

На практике механизм борьбы с указанными преступлениями имеет правовую основу в виде законопроектов или подзаконных актов.

Так, для минимизации угрозы телефонного мошенничества для российских граждан предлагается обязать операторов связи блокировать вызовы, приходящие из-за границы, но имеющие российскую городскую нумерацию. Часть вызовов от мошенников инициируется через VoIP-провайдеров, расположенных за пределами Российской Федерации. При этом мошенники указывают в подставляемом номере код города 495 или 499. Смысл этой меры – запретить операторам принимать или пропускать звонки от зарубежных VoIP-провайдеров, где номер телефона абонента, инициировавшего вызов, указан в российской нумерации (за исключением абонентов в роуминге).

Необходимо обязать операторов связи верифицировать телефонный номер при входящем вызове и блокировать вызовы, не прошедшие верификацию. При получении звонка на своего абонента оператор должен запросить у оператора, чей абонент инициировал вызов, действительно ли этот абонент сейчас совершает вызов, и если нет, то такой звонок на абонента не пропускать. Установить ответственность операторов связи за модификацию телефонного номера и нарушение требований постановления Правительства Российской Федерации от 28.03.2005 № 161 «Об утверждении Правил присоединения сетей электросвязи и их взаимодействия».

Необходимо ввести штрафы для операторов за то, что их абоненты или же они сами занимаются подменой номеров или используют для звонков номера, которые им не принадлежат, или же эти номера принадлежат другим операторам.

Целесообразно вернуться к рассмотрению ответственности операторов связи за нарушения требований по защите от подмены номера.

Повысить эффективность контроля исполнения законодательства Российской Федерации в части соблюдения условий лицензирования, правил оказания услуг связи, правил присоединения и правил пропуска трафика. Установить ответственность для

организаторов шлюзов по нелегитимному пропуску международного трафика под видом национального.

Следует провести анализ регулирования при взаимодействии IP и телефонных сетей и разработать необходимые изменения[1].

Пресечь рост киберпреступности можно посредством блокировки основного метода распространения киберпреступлений. Избавившись от вирусов, шпионского программного обеспечения и программ-вымогателей с помощью современного и эффективного антивируса, можно не только защитить свой компьютер от вредоносной программы, но и пресечь попытки злоумышленников получать выгоду, в том числе финансовые средства, противозаконно, что является их основной мотивацией.

К числу рекомендаций по предупреждению киберпреступлений следует отнести использование лицензионного программного обеспечения для защиты от заражения компьютера или мобильного устройства при установке различных программ; установление антивирусной программы не только на персональный компьютер, но и на смартфон, планшет и другую собственную компьютерную технику; не загружать файлы из непроверенных источников; использовать сложные пароли, состоящие из комбинаций цифр и букв или иных символов; не применять пароли, состоящие из дат рождения, имен, фамилий, т.е. те, которые легко вычислить либо подобрать.

Только совместными усилиями граждан и эффективными нормами законодательства можно сократить киберпреступность.

[1] *Берегитесь* телефона. URL: https://rg.ru/2021/02/14/kak-protivostoiat-kiberprestupnosti.html.

И.В. Горошко,
заведующий отделом
Университета прокуратуры
Российской Федерации,
доктор технических наук,
профессор

Некоторые подходы к гармонизации национальных уголовных законодательств в сфере противодействия компьютерной преступности

При всех преимуществах, которые предоставляет современная цифровая инфраструктура, можно утверждать, что развитие коммуникативных связей, интернет-технологий, глобализация информационного пространства существенно ослабили уровень защищенности общества от преступных посягательств.

Как подчеркивается в Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 05.12.2016 № 646, возможности трансграничного оборота информации, и прежде всего сети «Интернет», все чаще используются для достижения террористических, экстремистских, криминальных и иных противоправных целей, увеличивают масштабы и скоординированность компьютерных атак на объекты критической информационной инфраструктуры, способствуют нарастанию угроз суверенитету, территориальной целостности, политической и социальной стабильности Российской Федерации.

Аналогичные выводы с учетом национальной специфики содержатся во многих документах, определяющих направления развития кибербезопасности в странах Европейского союза, США, Канады, Японии и т.д.

В частности, в Национальной стратегии кибербезопасности Великобритании на период 2016–2021 гг. говорится о том, что киберпреступники расширяют область и стратегические методы своей преступной деятельности с целью получения большей выгоды от атак на британских граждан, организации и институты.

В Стратегии кибербезопасности Германии отмечается возросшая уязвимость информационных инфраструктур не только государственного и частного секторов, но и общества в целом.

Таким образом, при решении задач противодействия компьютерной преступности должны учитываться факторы транснационального характера и проходящие глобализационные процессы.

Отмеченные факторы обусловливают необходимость выработки единых подходов к отражению в уголовных законодательствах разных стран феномена компьютерной преступности.

В данном направлении предпринят ряд усилий, которые привели к разработке Конвенции о преступности в сфере компьютерной информации (Будапешт, 23 ноября 2001 г.) (далее – Конвенция).

Как подчеркивали разработчики данного документа, его главная цель состоит в том, чтобы обеспечить большую согласованность положений внутреннего уголовного права и сделать возможным использование эффективных средств расследования преступлений в сфере компьютерной информации путем совершенствования международного сотрудничества.

Для этого Конвенцией рекомендовано национальным уголовным законодательствам считать преступными следующие деяния:

преступления против конфиденциальности, целостности и доступности компьютерных данных и систем (противозаконный доступ (ст. 2); неправомерный перехват (ст. 3); воздействие на данные (ст. 4); воздействие на функционирование системы (ст. 5); противозаконное использование устройств (ст. 6);

преступления, связанные с использованием компьютерных средств (подлог с использованием компьютерных технологий (ст. 7); мошенничество с использованием компьютерных технологий (ст. 8);

преступления, связанные с содержанием данных (например, преступления, связанные с детской порнографией (ст. 9);

преступления, связанные с нарушением авторского права и смежных прав (ст. 10).

Аналогичный документ был подписан в Минске в 2001 г. государствами – участниками Содружества Независимых Госу-

дарств. Он назывался Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации (далее – Соглашение № 1) и предписывал считать уголовно наказуемыми умышленные деяния, связанные в том числе с осуществлением неправомерного доступа к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети; созданием, использованием или распространением вредоносных программ, и ряд других.

В 2018 г. в Душанбе было подписано Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий (далее – Соглашение № 2), в котором перечень данных преступлений расширился за счет добавления таких составов, как:

хищение имущества путем изменения информации, обрабатываемой в компьютерной системе, хранящейся на машинных носителях или передаваемой по сетям передачи данных, либо путем введения в компьютерную систему ложной информации, либо сопряженное с несанкционированным доступом к охраняемой законом компьютерной информации;

распространение с использованием информационно-телекоммуникационной сети «Интернет» или иных каналов электрической связи порнографических материалов или предметов порнографического характера с изображением несовершеннолетнего;

распространение с использованием информационно-телекоммуникационной сети «Интернет» или иных каналов электрической связи материалов, признанных в установленном порядке экстремистскими или содержащих призывы к осуществлению террористической деятельности или оправданию терроризма;

изготовление в целях сбыта либо сбыт специальных программных или аппаратных средств получения несанкционированного доступа к защищенной компьютерной системе или сети.

Осуществляемые попытки сближения национальных законодательств не могут не вызывать одобрения. Вместе с тем и они

не свободны от критики. Так, в Конвенции под единый видовой объект преступления – общественные отношения в сфере компьютерной информации попадают деяния, в которых использование компьютерных технологий выступает в качестве способа совершения преступлений (преступления, связанные с содержанием данных; преступления, связанные с нарушением авторского права и смежных прав).

Очевидно, что в правоприменительной практике может встречаться пересечение этих категорий, например, когда мошенничество совершается путем несанкционированного доступа к компьютерным данным.

Даже в подразделе, посвященном преступлениям против конфиденциальности, целостности и доступности компьютерных данных и систем, наблюдается неоднозначность в определении отдельных составов.

Так, в ходе противозаконного доступа может осуществляться воздействие на данные с использованием троянских программ, червей и вирусов; воздействие на функционирование системы может осуществляться подменой IP-адресов или нападением на программное обеспечение и т.п.

Аналогичные вопросы возникают и при изучении соглашений о сотрудничестве государств – участников Содружества Независимых Государств.

Так, вызывает сомнение необходимость выделения в Соглашении № 2 в отдельные составы преступлений, совершенных посредством сети «Интернет», поскольку информационно-телекоммуникационные сети, на наш взгляд, являются лишь инструментом, повышающим отрицательный эффект от преступного деяния.

Здесь следует остановиться на позиции нашей страны по поводу упомянутых Конвенции и Соглашений. Российская Федерация не ратифицировала Конвенцию о преступности в сфере компьютерной информации по причине наличия в ней ст. 32, разрешающей трансграничный доступ к хранящимся на территории государства компьютерным данным.

Согласно распоряжению Президента Российской Федерации от 15.11.2005 наша страна оставляет за собой право ратифициро-

вать Конвенцию только в случае пересмотра пункта о трансграничном доступе к компьютерным системам.

Соглашение № 1 ратифицировано с оговоркой, касающейся запроса на оказание содействия при проведении оперативно-розыскных мероприятий и процессуальных действий при раскрытии и расследовании преступлений в сфере компьютерной информации.

«Российская Федерация оставляет за собой право отказать в исполнении запроса полностью или частично, если исполнение запроса может нанести ущерб ее суверенитету или безопасности»[1].

По Соглашению № 2 внутригосударственные процедуры еще не выполнены, поэтому в силу оно не вступило.

Достижение безопасности в любой сфере человеческой деятельности (и информационная сфера не является исключением) невозможно без применения мер уголовной репрессии, что подразумевает уточнение понятия «противоправность».

Здесь также следует отметить наличие разных подходов к пониманию противоправности. Согласно Будапештской конвенции любое государство имеет право при определенных обстоятельствах не привлекать виновных к уголовной ответственности за нарушения авторских прав. При этом комментирование данных обстоятельств сопровождается размытой формулировкой «при наличии у государства иных эффективных средств правовой защиты».

В то же время в Соглашении № 1 деяние, связанное с незаконным использованием программ для ЭВМ и баз данных, являющихся объектами авторского права, считается уголовно наказуемым без каких-либо оговорок только в том случае, если оно причинило существенный ущерб.

Эти и другие перечисленные примеры свидетельствуют о том, что задача гармонизации национальных законодательств в сфере противодействия компьютерной преступности на основе некоторых общих принципов еще далека от решения.

---

[1] Федеральный закон от 01.10.2008 № 164-ФЗ «О ратификации Соглашения о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации».

Международному сообществу предстоит пройти непростой путь с тем, чтобы выработать унифицированные стандарты к ее оценке, безусловно, с учетом национальных особенностей, страновых различий в культуре, образе жизни и организации общественного пространства.

Т.А. Диканова,
заведующий отделом
НИИ Университета прокуратуры
Российской Федерации, доктор
юридических наук, доцент

Цифровизация как фактор, способствующий предупреждению правонарушений в транспортной системе стран СНГ и ЕАЭС

В настоящее время цифровизация рассматривается как важнейший фактор совершенствования управления транспортом, обеспечения его безопасного функционирования. Цифровизация, как предполагается, приведет к снижению аварийности, производственного травматизма и экологических катастроф, уровня ручного труда на опасных участках перевозочного процесса, позволит контролировать нахождение персонала в опасных зонах, автоматически запрещать выполнение рискованных операций, отрабатывать действия по ликвидации аварий, отграничивать аварии от иных нарушений технологий, своевременно предупреждать серьезные последствия.

Цифровизация на транспорте, переход от концепции конкуренции к выстраиванию экосистем участников перевозочного процесса как сообщества взаимодействующих и взаимно дополняющих хозяйствующих субъектов и регуляторов – мировой тренд. Сложнейшие политические и организационные задачи цифровизации национальных транспортных комплексов уже практически решили Китай, Япония, Корея, их опыт используется Россией. Цифровизация обеспечит интеграцию российской транспортной системы в мировое транспортное пространство и

реализацию транзитного потенциала. Цифровизация – составляющая Комплексного плана модернизации и расширения магистральной инфраструктуры на период до 2024 года (КПМИ).

Транспорт – сфера, цифровизация которой в России будет осуществлена в первую очередь, где будут созданы транспортные экосистемы – бизнес-вертикали, соединенные в безопасную среду, внутри которой при использовании любого из предлагаемых сервисов, управляемых из единого контакт-центра, потребителям гарантировано качество и безопасность[1]. Создание экосистем – «составляющая» выживания в условиях обострившейся конкурентной борьбы и экономического кризиса. Так, ОАО «РЖД» связано с другими видами транспорта, транспортными компаниями стран СНГ и Евразийского экономического союза (ЕАЭС), участвующими в перевозках, в том числе по международным транспортным коридорам (МТК). В связи с этим поставлена задача цифровизации и создания экосистем МТК. Поскольку, по подсчетам аналитиков, к 2028 г. на Азию будет приходиться до 45% мировых торговых потоков, требуется развитие МТК «Восток – Запад» («Один пояс, один путь») и «Север – Юг»[2].

Активную позицию в цифровизации МТК заняла Евразийская экономическая комиссия (ЕЭК). В 2020 г. ЕЭК утверждена программа опытной эксплуатации «удостоверяющего центра службы доверенной третьей стороны интегрированной информа-

---

[1] URL: https://trends.rbc.ru/trends/industry/5f6c55219a79475398b841bd (дата обращения: 18.02.2021).

[2] Решением Высшего Евразийского экономического совета от 26.12.2016 № 19 дано определение евразийского транспортного коридора. Это совокупность маршрутов, интегрированных в том числе в сеть МТК, проходящих по территориям государств-членов и обеспечивающих перевозки пассажиров и грузов в международном сообщении на направлениях их наибольшей концентрации, а также совокупность технологических и организационно-правовых условий осуществления этих перевозок. Комитетом по внутреннему транспорту Европейской экономической комиссии ООН дано следующее определение МТК – это часть национальной или международной транспортной системы, которая обеспечивает международные грузовые и пассажирские перевозки между отдельными географическими регионами, включает в себя подвижной состав и стационарные устройства всех или отдельных видов транспорта, работающих на данном направлении, а также совокупность технологических, организационных и правовых условий осуществления этих перевозок. «Международный транспортный коридор – наличие автомобильного, железнодорожного, водного и смешанных видов транспорта, которые осуществляют свою деятельность в непосредственной близости друг от друга или удаленных на многие километры, но ориентированных в одном общем направлении».

ционной системы». Эта служба – ключевой элемент процесса цифровизации ЕАЭС, а также организации трансграничного электронного документооборота в рамках этого союза. Создается Дирекция МТК, которая должна скоординировать управленческие решения органов власти, институтов развития и бизнеса. Подготовлен проект маршрутной сети из 10 МТК, наиболее перспективными их которых являются «Европа – Западный Китай», «Север – Юг», «Севморпуть», «Транссиб и БАМ»[1].

Цифровизация на транспорте – актуальный вопрос для СНГ. В решении Экономического совета СНГ от 15.09.2020 проанализированы итоги реализации Стратегии экономического развития СНГ на период до 2020 года и проект плана мероприятий по реализации первого этапа (2021–2025 гг.) новой такой Стратегии на период до 2030 г. В проекте плана предусмотрен специальный раздел о цифровизации, в том числе в транспортной и экспортной сферах, которая одной из своих целей имеет повышение взаимосвязанности пространства СНГ. Указанная Стратегия в части цифровизации МТК согласуется с принятыми ранее Стратегией обеспечения транспортной безопасности на территориях государств – участников СНГ при осуществлении перевозок в международном сообщении и Концепцией антитеррористической деятельности на железнодорожном транспорте государств – участников СНГ.

Цифровизация МТК предусматривает связность различных видов транспорта, транспортной системы с системой таможенных органов СНГ и ЕАЭС, между государственными платформами транспортных комплексов стран СНГ и ЕАЭС, системами взимания платы за использование объектов транспортной инфраструктуры, коммерческими логистическими платформами и экспедиторскими сервисами, автоматизированными системами перевозчиков и сервисами логистических центров, финансовыми и страховыми сервисами, технологиями спутниковой навигации, информационно-управляющими системами складской логистики, мониторинга и диспетчеризации перевозок. Требуется также разработка стандартов и модернизация существующих информаци-

[1] URL: http://www.eurasiancommission.org/ru/nae/news/Pages/19-06-2019-2.aspx (дата обращения: 18.02.2021).

онных систем. Требуется наладить эффективное взаимодействие перевозчиков и грузовладельцев, операторов транспортного комплекса во всех государствах – членах ЕАЭС, а также из третьих стран, установить особенности цифровизации для каждого вида транспорта (например, на автотранспорте умные светофоры на пешеходных переходах, что предупредит аварии на переездах и переходах – одна из наиболее актуальных проблем в настоящее время, устройства для водителей, сообщающие об опасностях на дороге и возможностях минимизировать пробки, и т.д.)[1].

Решение этих задач предусматривает обеспечение качества и безопасности транспортного комплекса, профилактику аварий. Отдельная проблема – цифровой мониторинг и контроль использования беспилотных технологий, обеспечение их безопасного функционирования. Профилактика аварий будет осуществляться с помощью выявления удобных маршрутов и условий транспортировки и декларирования грузов, использования электронных документов, оптимизации функции государственного контроля, бронирования очередности прохождения пограничного и таможенного контроля на международных пунктах пропуска.

Разработаны важнейшие нормативные акты, утверждены планы цифровизации, установлены показатели, отражающие внедрение цифровизации в транспортный комплекс страны[2], утверждены методики проведения статистической оценки уровня цифровизации[3]. Созданы подразделения, ответственные за реализацию проектов цифровизации: в Минтрансе – Департамент цифровой трансформации, в Ространснадзоре – Управление программ развития, цифровизации, информатизации и аналитики.

Процессы цифровизации на транспорте сопровождаются цифровизацией в сфере экспорта[4], что важно учитывать транспортным прокурорам, осуществляющим надзор за исполнением законов как в сфере транспорта, так и в таможенной сфере и сфере ВЭД. Предусмотрено издание необходимых для реализации

---

[1] URL: https://index1520.com/upload/medialibrary/b9c/Transportnie_koridori.pdf (дата обращения: 18.02.2021).

[2] Приказ Ространснадзора от 16.03.2018 № ВБ-184фс.

[3] Приказ Минтранса России от 17.06.2020 № 207.

[4] Общенациональный план действий, обеспечивающих восстановление занятости и доходов населения, рост экономики и долгосрочные структурные изменения в экономике (одобрен Правительством РФ 23.09.2020, протокол № 36, раздел VII).

планов цифровизации нормативных правовых актов, обеспечение экспортерам возможности пользования единой системой электронного документооборота, перечнями государственных и иных услуг (функций), административных и иных процедур в сфере ВЭД с помощью информационной системы «Одно окно». Формирование правовой базы для решения задач цифровизации в сфере экспорта осуществляется на базе цифровой платформы АО «Российский экспортный центр».

Имеются серьезные риски для реализации планов цифровизации транспорта в России. Коронакризис особенно мощно ударил по транспорту, прежде всего, воздушному, поставив его на грань выживания; внес коррективы в планы, в том числе в нацпроект «Транспортная часть комплексного плана модернизации и расширения магистральной инфраструктуры на период до 2024 года». Около половины расходов на проекты КПМИ – ответственность частных инвесторов, и существуют риски их отказов от реализации мероприятий. Для некоторых федеральных транспортных проектов возросли риски в связи со сложной ситуацией в экономике, снижением объемов перевозок, что, например, относится к федеральному проекту «Северный морской путь». Цифровизация МТК упирается в неразвитость паромных и контейнерных перевозок, снижение проходимости судов по внутренним водным артериям России и в ухудшение ситуации акваторий ряда портов, необходимость перераспределения грузопотоков с внутреннего водного, железнодорожного на автотранспорт, что требует активизации внимания к обеспечению безопасности автоперевозок. В связи с этим представляется необходимым усилить надзор за исполнением законов на автотранспорте, передав надзорные полномочия от территориальных транспортным прокурорам, учитывая тем более связность различных видов транспорта при цифровизации. Риском является старение российских транспортных объектов, отсутствие инфраструктуры, обеспечивающей работу беспилотного транспорта, недостаточное финансирование развития транспорта. По оценкам специалистов, в первую очередь это относится к МТК «Европа – Западный Китай» и трассе Москва – Казань.

Не только российские, но и мировые специалисты отмечают особую опасность для транспорта киберугроз, вмешательств в

систему управления транспортом, способных вызвать аварии, а также незаконное использование персональных данных пассажиров и клиентуры. Каждый вид транспорта имеет специфические угрозы кибератак. Например, объекты интеллектуальных систем на автотранспорте часто размещаются на обочинах дорог и автомагистралей, что дает преступникам возможность взаимодействовать с датчиками, портами и различными антеннами. Под угрозой находится интерфейс CAN – сеть контроллеров, которую «умные» автомобили используют для взаимодействия между собой. Возможен взлом беспроводных систем взаимодействия V2V, V2I и I2I, также обеспечивающих обмен данными при этом взаимодействии. Уязвимость в системах транспортных средств и незашифрованных сетях Wi-Fi может быть использована для перехвата управления транспортными средствами. Слабые пароли, незащищенные сайты и уязвимости в приложениях способны дать хакерам доступ к учетным данным пользователей и позволить, например, запустить или остановить двигатель транспортного средства удаленно. Для взлома может быть использована уязвимость голосового помощника в «умных» автомобилях. Перехват управления над 20% таких автомобилей может парализовать трафик. Использование вредоносного программного обеспечения способно полностью остановить работу целых секторов транспортной инфраструктуры. Устранение последствий таких атак влечет колоссальные расходы, потерю доходов, хищения собственности, включая транспортные средства. Возможны акты вмешательства, вызывающие включение систем аварийного оповещения. В 2017 г. несовершеннолетний хакер в США включил одновременно 156 таких систем. Киберпреступником может оказаться, например, автомеханик в мастерской, обслуживающий автомашину. Поскольку в ближайшие десятилетия на дорогах появится множество подключенных к сети «Интернет» транспортных средств и автомобилей-роботов, есть угрозы в связи с перебоями в работе сети.

По оценкам специалистов, на железнодорожном транспорте низший, средний и верхний уровни управления могут быть подвержены киберугрозам. На нижнем уровне управления возможны угрозы для умных станций и локомотивов. На среднем – атака на автоматизацию управления и маршрута. На верхнем – случаи

внедрения вредоносного софта и ссылок. Атаки возможны на связевые, энергетические системы и системы диагностики.

На воздушном и морском транспорте используются многочисленные информационные системы и технологии, некоторые из них в обязательном порядке устанавливаются на судах. Например, на морском транспорте функционируют идентификационная, картографическая, навигационная система автоматизации процессов, происходящих с грузами в порту; система, позволяющая отслеживать движение контейнеров посредством GPS и других каналов передачи данных; аварийный радиобуй; передатчик, подающий при активации сигнал бедствия, и т.д. Кибератаки на эти системы могут вызвать перехват и подмену информации или глушение того или иного сигнала. У компаний для передачи данных между трекерами, спутниками и наземными станциями отсутствуют механизмы аутентификации и шифрования, обслуживающие работу систем, а механизм передачи данных, работающий только в одну сторону, не предоставляет возможности валидации переданных данных. Спутниковые системы связи (SATCOM), в том числе связывающие через сеть «Интернет» суда друг с другом и с «большой землей», также содержат большое количество уязвимостей. Проверка терминалов спутниковой связи, используемых в судоходстве, выявила такие критические бреши в безопасности, как использование устройствами незащищенных или даже недокументированных протоколов, возможность эксплуатирования функции сброса пароля, бэкдоры[1].

Кибератаки способны отклонить от курса морские суда. Такой «эксперимент» с помощью имитатора GPS-сигналов, дублируя сигнал настоящего спутника и постепенно повышая мощность, проделали американские студенты, и им удалось «убедить» навигационную систему судна принимать сообщения спуфингового устройства и отбрасывать сигнал настоящего спутника как помехи. После того как навигационная система начала ориентироваться по данным двух спутников и атакующего устройства, судно отклонилось от первоначального курса.

---

[1] Бэкдор, тайный вход – дефект алгоритма, который намеренно встраивается в него разработчиком и позволяет получить несанкционированный доступ к данным или удаленному управлению операционной системой и компьютером в целом.

Возможны следующие сценарии: изменение данных о судне, включая его местоположение, информации о грузе, скорости и названии судна; создание «кораблей-призраков», опознаваемых другими судами как настоящие суда в любой локации мира; отправка ложной погодной информации конкретным судам, чтобы заставить их изменить курс для обхода несуществующего шторма, активация ложных предупреждений о столкновении, создание несуществующих поисково-спасательных вертолетов; фальсификация сигналов. Пираты уже злоупотребляют наличием прорех в системе кибербезопасности для планирования краж конкретных грузов.

Отдельно следует отметить такую угрозу для российской транспортной системы, как использование готовых зарубежных, прежде всего американских, технологий, которые активно продвигаются на рынке заинтересованными структурами. Известный специалист в области IT-технологий И. Ашматов указывает, что, если ими воспользоваться, через 5–7 лет значительно повысится уровень цифровой колонизации. Например, казалось бы, хорошо, когда датчики стоят на всех устройствах, позволяют контролировать транспорт, но проблема в том, что в России нет собственного стандарта на эти датчики. И датчики, и серверы, их обрабатывающие, в основном производятся на Западе. Наши автоматизированные системы управления уязвимы, работают на западных технологиях, управляются западным программным обеспечением. Своих систем в России практически нет. Кроме того, никто не проверял последствия возможного одновременно с отключением интернет-маршрутизации извне отзыва сертификатов шифрования. Если это сделать, весь транспорт встанет. В России практически 100% процессоров, маршрутизаторов и т.д. западного производства. Какие в них «закладки» и средства удаленного управления, мало кто знает. Некоторые системы критичного применения проверяются, но далеко не все. Российский рынок интернет-проектов и программного обеспечения составляет всего 2% от мирового. И. Ашманов сослался на киберстратегию США, в которой сказано: открытый общедоступный Интернет – «это средство продвижения американских ценностей по планете, и если кто-то из врагов США, «авторитарных режимов», прикрываясь ложным понятием суверенитета или информационной безопасно-

стью, будет ограничивать Интернет на своей территории, мы его накажем как киберсредствами, так и обычными инструментами: политики, экономики и войны». В связи с этим напрашивается вывод: цифровизации должно предшествовать импортозамещение. И кроме того, импортозамещение нужного масштаба – это дело государства, а не частных компаний[1].

Общими для всех видов транспорта угрозами являются отказ критических IT-систем, зависимость от сторонних поставщиков и их уязвимость, усложнение правил и транспортных технологий при сокращении численности персонала благодаря цифровизации, недостаточная активность в части внедрения новых технологий, потеря доходности перевозок из-за необходимости внедрения таких технологий, угрозы от новых конкурентов, чрезвычайная зависимость от национальной транспортной инфраструктуры, геополитическая нестабильность и неопределенность.

Недостаточное внимание к защите от угроз в транспортной сфере может стать причиной перехвата управления и сбоев в работе транспорта. Специалисты также отмечают, что далеко не вся информация о кибератаках получает широкую огласку: часто владельцы бизнеса замалчивают ее, опасаясь таких последствий, как потеря имиджа, претензии со стороны клиентов и страховых компаний, проведение расследований. Дополнительный риск – отсутствие общего регулирования и стандартизации информационных систем в транспортной отрасли – затрудняет цифровизацию и киберзащиту.

Вместе с тем ведется разработка средств предупреждения кибератак. Это меры физической защиты объектов транспортной инфраструктуры, запрет доступа посторонних лиц, контроль за сотрудниками, запрет проноса на транспортный объект цифровых гаджетов, исключая необходимые для техобслуживания, применение сегментирования сетей, отслеживание их состояния и использование систем обнаружения и блокирования вторжений, регулярный аудит на предмет уязвимостей сети, оборудования и программного обеспечения или прошивок и т.д.[2] Международные транспортные организации принимают меры, направленные на

---

[1] *Ашматов И.* Новый виток цифровой колонизации. URL: https://www.youtube.com/watch?v=uuwQCPsOLwU (дата обращения: 18.02.2021).

[2] URL: https://habr.com/ru/company/trendmicro/blog/492018/(дата обращения: 18.02.2021).

предупреждение кибератак, например, Международная морская организация (ИМО)[1].

Цифровизация на транспорте сопровождается цифровизацией управления и контроля, изменениями в формировании источников информации о состоянии транспорта и экспорта, созданием вместо прежних новых органов управления и контроля. Цифровизация обеспечивает информационное обслуживание государственных контролирующих органов в сфере транспорта и международной торговли, создание цифровых интеллектуальных систем контроля, ведение нормативно-справочных баз, мониторинг ситуации на транспорте, интеграцию с Единым порталом государственных и муниципальных услуг. Совершенно очевидно, что в связи с этим требуется корректировка организации и методики осуществления прокурорского надзора за исполнением законов на транспорте, цифровизация в системе правоохранительных органов, в том числе транспортной прокуратуры, и новые технологии, внедряемые здесь, должны быть сопряжены с применяемыми на транспорте информационными системами.

[1] ИМО приняла Приложение № 10 – Резолюция КБМ ИМО MSC.428(98). Резолюция – настоятельно рекомендует администрациям обеспечить надлежащее рассмотрение киберрисков в системах управления безопасностью не позднее первой ежегодной верификации документа о соответствии компании требованиям безопасности после 01.01.2021. Разработаны Рекомендации по управлению киберрисками в морской отрасли (циркуляр КБМ-ФАЛ (MSC-FAL./Circ. 3). Отмечается необходимость в первую очередь уделить внимание вопросам стандартизации и законодательного регулирования процесса внедрения информационных систем на транспорте. URL: https://safe.cnews.ru/news/top/2018-01-04_risk_kiberatak_na_transportnuyu_infrastrukturu (дата обращения: 18.02.2021).

Е.В. Кунц,
ведущий научный сотрудник НИЦ-3
НИИ ФСИН России, доктор
юридических наук, профессор

Зарубежный опыт противодействия преступлениям в сфере телекоммуникационных технологий

Характерной особенностью данных преступлений является то, что потерпевшим от преступлений может стать любой человек, имеющий банковский счет, привязанный к банковской карте.

Учитывая, что мошенники совершают серию однотипных преступлений, эффективность раскрытия и расследования указанных преступлений напрямую зависит от своевременного сообщения потерпевшими обо всех обстоятельствах совершения преступления.

Чтобы не стать жертвой мошенников, надлежит придерживаться следующих советов: нельзя распространять реквизиты банковский карты. Банк не имеет права требовать данные пластиковой карты. Для того чтобы проверить поступившую информацию о блокировании карты, необходимо позвонить в клиентскую службу поддержки банка. Если поступило предложение от радиостанции активировать карточки экспресс-оплаты с целью получения приза, включите радиостанцию и прослушайте ее эфир, радиостанция никогда не требует активировать карточки экспресс-оплаты при проведении лотереи[1].

Преступления в данной сфере распространены в зарубежных странах (например, в Великобритании с конца 90-х гг. прошлого столетия). Мошенничество на линиях телекоммуникаций во всемирном масштабе ежегодно наносит ущерб в размере примерно 30 млрд долл. После изобретения персональных компьютеров и создания международной сети «Интернет» стало просто получить сведения, необходимые для совершения мошенничества на линиях телекоммуникаций. В настоящее время в этой об-

[1] Виды преступлений, совершаемых с использованием информационно-телекоммуникационных технологий. URL: https://06.мвд.рф/news/item/19364411 (дата обращения: 12.02.2021).

ласти используются хорошо организованные и изощренные методы мошенничества.

Существует широкий круг преступлений на линиях телекоммуникаций, которые варьируются от краж телекоммуникационного оборудования до более сложных видов мошенничества. В систему телефонной связи госпиталей Великобритании было произведено вторжение хакеров, осуществивших за выходные дни международные телефонные разговоры на 69 тыс. долл., за которые платить пришлось госпиталям.

Работники систем телекоммуникаций разработали свой язык для сферы мошенничества.

Телефонный фрикер является вариантом компьютерного хакера в применении к телефонной связи. Телефонные фрикеры впервые появились в конце 60-х – начале 70-х гг. прошлого столетия, они подключаются к телефонной сети с помощью различных методов. Намерения фрикера не всегда преступны, иногда он вторгается в телефонную сеть, чтобы проверить разработанный им вариант подключения к телефонной линии.

Черный ящик позволяет хакеру получить услуги телекоммуникационной компании бесплатно. Он может быть спроектирован так, что дает возможность свободно принимать входящие телефонные звонки, подавлять информацию о счетах за телефонные разговоры, которые нужно оплатить, получать доступ к телефонной линии пользователя или осуществлять свободные вызовы с телефонного аппарата, который срабатывает от монеты.

Клонинг – это кража электронной идентификационной системы мобильного телефона и внедрение этой системы в другой мобильный телефон, что позволяет осуществлять телефонные переговоры с мобильного телефона за счет другого пользователя сотовой телефонной связи.

Продажа телефонных вызовов дает возможность осуществлять телефонные переговоры по заниженным тарифам. Данный тип мошенничества часто встречается в общинах этнических меньшинств, члены которых остро нуждаются в телефонных переговорах со своими родственниками и знакомыми, живущими в заморских странах.

Обман при открытии счета – в этом случае мошенник под чужим именем открывает счет в телекоммуникационной компа-

нии, предполагая, что за телефонные разговоры будет платить носитель данной фамилии. Такие счета часто используются как база для так называемой продажи телефонных вызовов и для других нелегальных манипуляций.

Обман с использованием премиального телефонного номера предоставляет самые разнообразные услуги, создавая возможности для этого вида обмана. Мошенник маскируется под телефонным номером и получает выплаты от телекоммуникационной компании.

Обман с использованием предоплаты предполагает, что мошенник получает услуги телекоммуникационной компании путем обманного использования украденных кредитных карточек.

Обман с использованием частной телефонной сети характеризуется тем, что мошенничество осуществляется в разных формах путем получения нелегального доступа к частным телефонным линиям и к системе речевой почты. В этом случае мошенник стремится осуществить телефонный разговор за счет владельца частной телефонной станции.

В 1999 г. Министерство финансов Великобритании сообщало, что ряду организаций общественного сектора экономики нанесен существенный ущерб от мошенничества на линиях телефонной связи. Один случай такого мошенничества, реализованный на линиях частной телефонной сети, принес убытки в 80 тыс. долл. в день, а другой случай – ущерб в 640 тыс. долл. в течение шестинедельного периода.

В ходе акта мошенничества, зарегистрированного в 1999 г., преступники подкупили с помощью взяток служащих телекоммуникационной сети для того, чтобы иметь возможность тайно считывать информацию с линий связи между банковской кассовой машиной и центральным компьютером банка. Собранная информация затем вводилась в персональный компьютер с намерением перевести детали счетов клиентов банка на новые банковские пластиковые карточки, которые предполагалось использовать для незаконного снятия денег с чужих счетов.

Развитие кабельных линий связи, используемых не только для передачи сообщений, но и для развлекательных целей, привело к тому, что произошло практически массовое распространение так называемых нелегальных ящиков, спроектированных для

получения кинофильмов, спортивной и другой информации развлекательного характера в обход системы оплаты этих услуг. Данный вид мошенничества ежегодно наносит ущерб в размере многих сотен тысяч фунтов стерлингов владельцам кабельных сетей связи в Великобритании, а недавно были раскрыты целые подпольные фабрики по изготовлению нелегальных ящиков.

Председатель форума по борьбе с мошенничеством на линиях коммуникаций Великобритании заявил, что «операторы телекоммуникационных линий Великобритании выигрывают борьбу с мошенниками, действующими на линиях телекоммуникаций, и что ущерб от мошенничества на этих линиях страны значительно ниже усредненного международного уровня ущерба от данного вида преступной деятельности»[1].

Английская телекоммуникационная индустрия давно признала, что для снижения уровня финансового ущерба от мошенничества и других видов преступной деятельности на линиях телекоммуникаций необходимо осуществить ряд мер, которые позволяли бы не только обнаруживать преступления на линиях телекоммуникаций, но и заранее предупреждать пользователей о том, что на данной линии телекоммуникаций может быть совершено преступление.

Нет единого решения данной проблемы, для решения всех этих проблем нужно сочетание методов и процедур. Достижения в области персональных компьютеров сделали для мошенников привлекательными перспективы актов мошенничества на линиях телекоммуникаций, но в то же время еще более совершенные достижения в компьютерной технологии сделали возможным осуществление мероприятий, позволяющих выявлять эти нарушения.

В настоящее время на линиях телекоммуникаций можно установить системы, которые позволяют наблюдать в реальном времени за деятельностью легальных пользователей телекоммуникационных линий связи и сразу выявлять нелегальных пользователей до того, как те успеют нанести существенный материальный ущерб телекоммуникационной компании. С помощью подобных систем можно не только выявлять мошенника, но и предъявлять ему обвинение по поводу нанесенного им матери-

[1] Intersec. 1999. October. P. 307–310.

ального ущерба. Компьютерные распечатки о материальном ущербе, причиненном мошенником, можно использовать в качестве судебных доказательств.

Достаточно сложно оценить масштаб материальных потерь, наносимых мошенниками на линиях телекоммуникаций. Телекоммуникационные компании неохотно оглашают сведения о размере ущерба, причиненного мошенничеством, так как это свидетельствует о слабости мер безопасности на линиях телекоммуникаций. Однако среди специалистов принято считать, что мошенники наносят ущерб в размере примерно от 3 до 8% от прибыли.

Телекоммуникационные компании обмениваются между собой информацией о методах, используемых мошенниками. В рамках телекоммуникационной индустрии создан ряд специализированных организаций, которые занимаются распространением подобной информации. Данная информация позволяет сократить масштабы мошеннической деятельности. Мошенники быстро выявляют уязвимые места в линиях телекоммуникаций, и недавние случаи незаконного использования кредитных карточек для получения возможности практически бесплатно вести телефонные разговоры свидетельствуют об этом.

Привлечь преступника, действующего на линии телекоммуникаций, к уголовной ответственности не так просто, как это кажется. Поэтому индустрия телекоммуникаций стремится к удалению некоторых положений из системы уголовного правосудия, которые иногда не позволяют привлечь к уголовной ответственности конкретного мошенника. Правовые вопросы, связанные с функционированием линий телекоммуникаций в Великобритании, регулируются законом о телекоммуникациях от 1984 г.

Мошенничество и другие виды преступлений в сфере телекоммуникаций не всегда ограничиваются одной страной, в данном случае Великобританией, они имеют международный характер и охватывают все страны и континенты.

Подтверждением успешного противодействия преступникам является реализация схемы, предохраняющей от мошенничества в мобильной телефонной связи. В результате в 1998–1999 гг. в Великобритании были привлечены к уголовной ответственности 39 человек за преступления против индустрии телекоммуника-

ций, в одном случае к этим обвинениям были добавлены пункты по незаконному обороту огнестрельного оружия. Число людей, привлеченных к уголовной ответственности за мошенничество на линиях телекоммуникаций, было бы больше, если бы законы, регулирующие правовые вопросы функционирования коммуникаций, были согласованы с последними достижениями науки и техники. Большая часть дел, связанных с мошенничеством в области телекоммуникаций, рассматривается уголовными судами Великобритании в соответствии с законом о кражах от 1968 г. В настоящее время признано, что правовые нормы в отношении функционирования линий телекоммуникаций являются неадекватными и нуждаются в совершенствовании. Достижения науки и техники всегда будут опережать законы, регулирующие их использование[1].

В условиях усиливающейся конкуренции на рынке телекоммуникационных услуг появляются все новые способы совершения данных преступлений. Роль профессионала, специализирующегося на проблемах борьбы с мошенничеством на линиях телекоммуникаций, заключается в том, чтобы распознать мошенничество и обеспечить задействование всех средств борьбы с ним.

М.Ю. Дворецкий,
доцент кафедры правовых дисциплин
Российской академии народного хозяйства
и государственной службы
при Президенте Российской Федерации,
кандидат юридических наук, доцент

Направления совершенствования мер противодействия преступлениям в сфере компьютерной информации

Законодатель отказался от того, чтобы конкретно указывать и перечислять все технические средства, на которых может находиться охраняемая законом компьютерная информация.

[1] Intersec. 1999. October. P. 307–310.

Статья 273 УК РФ предполагала назначение умышленно действовавшему виновному лишь трехлетнего срока лишения свободы (ч. 1), при наличии квалифицированных обстоятельств – от трех до семи лет (ч. 2), тем самым алогично наказывая за неосторожную форму вины, т.е. легкомысленно или небрежно при достигнутых последствиях, что фактически отражало несовершенство данной конструкции и пробел в юридической технике, требовавший устранения. Поскольку констатируется наличие систематических сложностей с восприятием правоприменителями содержания вредоносной компьютерной программы из-за первоначально предполагавшегося широкого трактования посредством несанкционированных ее действий, которые не одобрил пользователь, последующего отнесения к ним по заключению программно-технической экспертизы направленных на модификацию. Изначально они содержат функциональный набор, потенциально способный из-за выполнения определенных манипуляций привести к вредным последствиям, несмотря на их легальность и законопослушность пользователей. В профессиональном сообществе этимология понятия «компьютерная программа» подразумевает ее условную опасность посредством возможного вреда в дальнейшем для потенциального потерпевшего. Скорректированная ст. 274 УК РФ по-прежнему оставляет актуальной проблемой квалификации уголовно-правовую оценку нарушения правил эксплуатации.

Согласно ст. 2 Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» фактически выступают объекты, непосредственно относящиеся к здравоохранению, транспорту, банковской сфере, оборонному комплексу, атомной энергетике, топливно-энергетическому комплексу и т.д. Объективную сторону посягательств образуют действия. Преступление считается фактически оконченным с момента, когда виновным был непосредственно нанесен вред.

Состав преступления, предусмотреного ч. 3 ст. 274^1 УК РФ, характеризуется виной в виде прямого либо косвенного умысла, легкомысленно либо небрежно. Посягающий, осознавая характер и степень общественной опасности нарушения правил эксплуатации средств хранения, обработки или передачи охраняемой ком-

пьютерной информации, хотя мог предвидеть возможное либо неизбежное причинение вреда, желая именно этого или не желая, но осознано допуская либо относясь безразлично; либо не желая, без достаточных на то оснований рассчитывает на их предотвращение (легкомыслие); либо не предвидя виновным возможности наступления. Поскольку общественно опасное содеянное (ч. 3 ст. 274[1] УК) виновным предполагает его умышленную форму вины либо неосторожность, когда, предвидя нарушения правил эксплуатации, но без достаточных к тому оснований, самонадеянно рассчитывает на предотвращение последствий либо не предвидит указанных в законе последствий, хотя при необходимой внимательности и предусмотрительности должен был и мог предвидеть.

Неквалифицированное содеянное предполагает назначение принудительных работ на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового либо лишение свободы на срок до шести лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового. Общественная опасность посягательства возрастает по экспоненте, конструкция статьи с уточняющим квалифицирующим признаком максимально индивидуализирует наказание и дифференцирует ответственность виновных. При этом следует учесть, что вследствие повышенной ответственности виновных соучастников, как и участие в ней (ст. 35 УК РФ), сформулированное законодателем в качестве отягчающего обстоятельства, назначаемые виды наказания соразмерны содеянному. Содержание обстоятельства «лицо, с использованием своего служебного положения» предполагает уголовную ответственность виновного как непосредственного исполнителя, так и его руководителя (ч. 4 ст. 274[1]). Преступления с использованием своего служебного положения и при этом организация группы соответственно наказываются согласно ст. 69 УК РФ.

Содержанием ч. 5 ст. 274[1] предусматривается не угроза наступления последствий (ст. 272–274 УК РФ), оцениваемых как тяжкие, а лишь факт их наступления. Современной судебной практикой не выработан единый подход для оценки содержания «тяжкие последствия», как правило, ограничиваемого определе-

нием размера в денежном эквиваленте. Каждое уголовное дело, рассматриваемое судом, предполагает установление фактического размера вреда/тяжести последствий непосредственно исходя из обстоятельств содеянного виновным и согласно существующей правоприменительной практике Российской Федерации. Априори неопределенность толкования размеров нанесенного потерпевшим ущерба, точное определение категории негативного последствия содеянного по-прежнему остается актуальной научно-практической проблемой. Вследствие того, что их этимология предполагает наличие факта наступления наиболее опасных последствий (причинение легкого или средней тяжести вреда здоровью, неосторожное причинение вреда здоровью, смерть). Санкция предполагает распространение на номенклатуру. Суд может проигнорировать назначение данного вида наказания, оставляя в первую очередь поле для судейского субъективизма.

И.В. Карлов,
старший преподаватель кафедры
управления и административно-правовых
дисциплин юридического факультета
ВЮИ ФСИН России, кандидат
юридических наук

Использование современных информационных технологий для противодействия преступности в местах лишения свободы

На расширенном заседании коллегии УФСИН России по г. Москве в 2020 г. директором ФСИН России А.П. Калашниковым в качестве приоритетных задач развития службы были обозначены обеспечение безопасности, а также оборудование учреждений современными интеллектуальными техническими средствами охраны, надзора и контроля[1]. Несмотря на возможные высокие затраты, данные задачи, безусловно, являются значимыми

[1] *Молчание* Бутырки. Тюремное ведомство апробирует системы точечного подавления мобильной связи в колониях и СИЗО. URL: https://rg.ru/2020/02/03/v-koloniiah-i-sizo-aprobiruiut-sistemy-tochechnogo-podavleniia-mobilnoj-sviazi.html (дата обращения: 10.02.2021).

и своевременными, поскольку диктуются все большей цифровизацией общественной жизни и переходом значительной части преступности в информационную среду, что требует современных технических средств противодействия данному опасному явлению. В рамках нашего исследования будет сделан небольшой обзор основных информационных систем и программных продуктов, используемых в уголовно-исполнительной системе, проблем применения и перспективных направлений их развития.

С 2012 г. эффективно применяется система электронного слежения (СЭМПЛ), которая стала одним из первых высокотехнологичных продуктов в УИС. Она представляет собой комплекс электронных устройств, в состав которого входят электронный браслет (надеваемый на щиколотку осужденного) и два контрольных устройства (стационарное находится в месте проживания осужденного, а мобильное выдается ему на руки с обязанностью брать всегда с собой или находиться на удалении не более пяти метров от контролируемого лица). Оба устройства имеют уникальный индивидуальный номер, занесенный в базу данных, и осуществляют непрерывный круглосуточный прием и обработку радиосигналов с электронного браслета. При этом мобильное контрольное устройство определяет место положения осужденного по сигналам системы ГЛОНАСС, а стационарное обеспечивает информационный обмен по GSM-каналам, что позволяет круглосуточно в автоматическом режиме отслеживать все передвижения осужденного во время его пребывания под домашним арестом и соблюдения им установленных судом ограничений. Кроме того, контрольные устройства оповещают подразделение ФСИН России о попытках снятия и повреждения браслета, длительном отсутствии движения, выходе за пределы охранной зоны и иных нарушениях[1].

Использование СЭМПЛ также во многом позволяет снизить нагрузку на исправительные учреждения за счет применения альтернативных видов наказаний, не связанных с лишением свободы, а также сотрудников уголовно-исполнительных инспекций по контролю за осужденными. В то же время стоимость устройств по-прежнему остается высокой (около 100 тыс. руб.), что затрудняет их массовое использование.

---

[1] Подробнее см.: *Система* электронного мониторинга подконтрольных лиц. URL: https://ria.ru/20130226/924751757.html (дата обращения: 12.02.2021).

Были выявлены и факты значительного искусственного завышения стоимости во время первоначальных массовых закупок, причинивших ущерб бюджету более чем на 2,7 млрд руб.[1] При этом качество полученных браслетов оставляло желать лучшего. По данным Счетной палаты Российской Федерации, по состоянию на 1 января 2018 г. из 52 663 ед. оборудования, предназначенного для функционирования СЭМПЛ, не использовалось 72,3% от общего количества, а 44,3% были вовсе неисправны, что свидетельствовало о неэффективном использовании имущества, на закупку которого были израсходованы средства федерального бюджета[2].

Следующей и наиболее широко используемой системой является федеральная государственная информационная система «Электронный документооборот уголовно-исполнительной системы» (ФГИС «СЭД УИС»), которая была введена в 2014 г. в целях повышения эффективности управления путем обеспечения безбумажного документооборота при внутренней организации деятельности ФСИН России и учреждений, непосредственно подчиненных ФСИН России. Кроме того, СЭД УИС обеспечивает защиту информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий. Это имеет особое значение в условиях участившихся атак на российские интернет-ресурсы.

Тем более что, по данным Национального координационного центра по компьютерным инцидентам (НКЦКИ), более трети (35%) таких атак направлены на хищение информации из систем государственного управления[3].

Кроме того, в России наблюдается повышение криминальной активности в сфере хищения персональных данных. Так, в 2019 г. объем украденных персональных данных граждан нашей страны вырос в 6,5 раза, скомпроментировано более 172 млн за-

---

[1] *История* уголовного дела экс-директора ФСИН Александра Реймера. URL: https://tass.ru/info/7830481 (дата обращения: 12.02.2021).

[2] Отчет о результатах контрольного мероприятия «Аудит эффективности использования государственных ресурсов на информатизацию Федеральной службы исполнения наказаний в 2015–2017 годах». С. 269. URL: https://ach.gov.ru/upload/iblock/6c5/6c5a1ce4612053f63eb1805aca2a0e26.pdf.

[3] *Центр* кибербезопасности рассказал про атаки на российские ресурсы из ЕС и США. URL: https://tass.ru/obschestvo/6599550 (дата обращения: 12.02.2021).

писей (что превысило число жителей нашей страны)[1]. Опасность состоит еще и в том, что персональные данные сотрудников УИС могут быть использованы криминальным элементом для оказания давления на персонал исправительных учреждений в целях склонения к совершению коррупционных преступлений и иных действий вопреки интересам службы.

Учитывая повышенную значимость, защита информации в ФГИС «СЭД УИС» построена на нескольких уровнях (подсистемах) и включает в себя ведомственную сеть связи, подсистемы идентификации и аутентификации пользователей, управление доступом логирования и делегирования полномочий[2]. К тому же в соответствии с п. 155 Инструкции по делопроизводству в учреждениях и органах уголовно-исполнительной системы, утвержденной приказом ФСИН России от 10.08.2011 № 463, работник, допущенный к передаче (приему) документов, несет персональную ответственность за соблюдение требований приема-передачи документов по каналам электрической связи. Кроме того, при передаче электронных документов в другие государственные органы документы заверяются электронной подписью руководителя учреждения или органа УИС, что дает дополнительную защиту информации.

Следует также отметить, что в настоящее время запрещается передавать в электронных сообщениях сведения, составляющие государственную тайну, и сведения с грифом «Для служебного пользования», что приводит к необходимости перевозки данных документов в бумажном виде сотрудниками специальной и фельдъегерской связи, что, естественно, снижает скорость передачи информации. Представляется, что с развитием средств защиты информации и каналов связи в уголовно-исполнительной системе удельный вес электронных отправлений будет только расти.

Важное значение в предупреждении пенитенциарной преступности имеют инженерно-технические средства охраны и надзора (ИТСОН), которые применяются с целью создания усло-

---

[1] *Данные* на ветер: количество утечек персональной информации выросло на треть. URL: https://iz.ru/1016433/anastasiia-gavriliuk/dannye-na-veter-kolichestvo-utechek-personalnoi-informatcii-vyroslo-na-tret (дата обращения: 12.02.2021).

[2] Подробнее см.: *Морозова О.Ю.* Федеральная государственная информационная система «Электронный документооборот уголовно-исполнительной системы» (ФГИС «СЭД УИС») и основные уровни защиты информации в ней // Актуал. вопр. информатизации Федеральной службы исполнения наказаний на соврем. этапе развития уголовно-исполнительной системы: сб. материалов круглого стола / ФСИН России. М., 2018.

вий для предупреждения и пресечения преступлений (в том числе побегов), нарушений установленного режима содержания осужденных и лиц, содержащихся под стражей, повышения эффективности надзора за ними и получения необходимой информации об их проведении, а также обеспечения выполнения других служебных задач, возложенных на учреждения и органы уголовно-исполнительной системы[1].

В условиях стремительного развития средств связи и коммуникации первостепенное значение приобретает ограничение контактов осужденных с внешней средой, что может быть использовано для координации преступной деятельности, облегчения проникновения запрещенных предметов, совершения преступлений с использованием мобильных телефонов (прежде всего мошеннических действий). Вопрос предупреждения совершения преступлений с использованием средств мобильной связи был даже вынесен на заседание коллегии ФСИН России в 2021 г.[2]

Значимую помощь в борьбе с данными преступлениями в исправительных учреждениях оказывают средства подавления сигналов мобильной связи. В то же время существующие технические системы обладают слишком сильным действием, что приводит к снижению качества связи в окружающих домах и организациях и служит причиной недовольства граждан. Поэтому ФСИН России принимаются меры по апробации технических систем более точечного подавления средств мобильной связи в исправительных учреждениях (на базе следственных изоляторов г. Москвы). Кроме того, чтобы повысить оперативность реагирования, предлагается использовать специальные металлодетекторы, способные выявлять спрятанные деньги и сим-карты. Также в рамках пилотного проекта предлагается оборудовать СИЗО г. Москвы дополнительными видеорегистраторами, камерами видеонаблюдения и рентгенотелевизионными установками, что обеспечит стопроцентное видеонаблюдение[3].

---

[1] Приказ Минюста России от 04.09.2006 № 279 «Об утверждении Наставления по оборудованию инженерно-техническими средствами охраны и надзора объектов уголовно-исполнительной системы». URL: https://base.garant.ru/70179058/ (дата обращения: 15.02.2021).

[2] План работы коллегии Федеральной службы исполнения наказаний на 2021 год. URL: https://fsin.gov.ru/structure/inspector/ОК/План%20работы%20коллегии%202021%20для%20сайта.pdf (дата обращения: 15.02.2021).

[3] URL: https://rg.ru/2020/02/03/v-koloniiah-i-sizo-aprobiruiut-sistemy-tochechnogo-podavleniia-mobilnoj-sviazi.html (дата обращения: 15.02.2021).

Важное значение имеет и принятие Федерального закона от 09.03.2021 № 44-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части прекращения оказания услуг связи на территории следственных изоляторов и учреждений, исполняющих уголовные наказания в виде лишения свободы», обязывающего сотовых операторов по запросам ФСИН России производить адресное отключение абонентских номеров, незаконно используемых осужденными в местах лишения свободы. Оказание услуг связи по абонентским номерам должно быть прекращено оператором связи на основании решения в письменной форме директора ФСИН России или его заместителя либо начальника территориального органа уголовно-исполнительной системы, в ведении которого находятся следственный изолятор или исправительное учреждение. Соответствующий порядок взаимодействия ФСИН России и его территориальных органов с операторами связи, а также форма решения о прекращении оказания услуг связи, сроки его принятия и направления операторам связи, сроки прекращения оказания услуг связи по указанным абонентским номерам устанавливаются Правительством Российской Федерации[1].

Также следует отметить, что в настоящее время ФСИН России совместно с корпорацией «Ростех» подготовлен масштабный план цифровизации уголовно-исполнительной системы стоимостью около 25 млрд руб., в рамках которого планируется внедрить в 380 исправительных учреждениях электронные системы документооборота, более совершенную систему видеонаблюдения с функцией распознавания лиц, разработать и модернизировать собственные IT-системы, закупить компьютерную технику, а также разместить средства блокировки мобильной связи после апробации в г. Москве[2].

Поскольку учреждения уголовно-исполнительной системы представляют собой целые жилищно-хозяйственные комплексы,

---

[1] Операторов обязали отключать сотовую связь в случаях выявления фактов использования абонентских номеров подозреваемыми, обвиняемыми и осужденными в СИЗО и исправительных учреждениях. URL: http://www.consultant.ru/law/hotdocs/67997.html/ (дата обращения: 15.06.2021).

[2] *В исправительных* учреждениях появятся системы распознавания лиц, новые IT-сервисы и оборудование. URL: https://fsin.ru/news/v-ispravitelnykh-uchrezhdeniyakh-poyavyatsya-sistemy-raspoznavaniya-lits-novye-it-servisy-i-oborudovanie (дата обращения: 21.02.2021).

оборудованные в инженерном отношении, к тому же нередко автономные и находящиеся на большом удалении от поселений, важное значение приобретает организация централизованного управления. В этом отношении важную роль играет автоматизированная система управления и диспетчеризации (АСУД) ФСИН России (была введена в эксплуатацию в 2013 г.). АСУД предназначена для удаленного отображения сбора и хранения данных о работе технологического оборудования здания или производственного процесса, централизованного мониторинга, диспетчеризации и управления оборудованием инженерных систем, информирования о нештатных ситуациях. Основное же назначение системы состоит в централизации контроля и управления исправительным учреждением. В то же время следует отметить, что система диспетчеризации не освобождает полностью сотрудника от принятия множества рутинных решений, так как, прежде всего, выводит информацию, а само решение принимается вручную оператором.

В этом отношении более перспективным является дальнейшее развитие системы с превращением ее в комплексную систему автоматизации BMS (Building Management System), с появлением своего рода «умных тюрем», в которых глубоко интегрированы все системы обеспечения на основе искусственного интеллекта. Правда, указанное направление требует больших затрат на модернизацию, что создает сложности в условиях ограниченности бюджетного финансирования, но позволит минимизировать пресловутый человеческий фактор. Это важно для профилактики коррупционных и должностных преступлений, традиционно составляющих около половины всех выявляемых преступлений сотрудников уголовно-исполнительной системы[1].

В борьбе с преступностью большое значение имеют накопление, анализ и обработка данных. Здесь на помощь приходят государственные информационные системы ФСИН России: АИС «Статистика «УИС», программные комплексы автоматизированного карточного учета лиц, содержащихся в исправительных учреждениях, поисковая информационная система подозреваемых, обвиняемых и осужденных «Паноктикум», электронная база данных судебных дел, информационная система «Розыск-контингент» и др.

[1] Сведения о преступлениях среди личного состава УИС: отчеты по форме ФСИН-7 (работа с личным составом) за 2016–20120 гг. Документы опубликованы не были. Доступ из автоматизированной информационной системы «Статистика ТО УИС».

По нашему мнению, в перспективе будет происходить их целенаправленная интеграция между собой и с информационными системами иных правоохранительных органов, что должно повысить скорость доступа и качество обработки данных.

Как видно, информационное оснащение уголовно-исполнительной системы является современным: к 2018 г. только в центральном аппарате ФСИН России использовалось 24 информационных системы или программных комплекса[1]. С учетом взятого курса на цифровизацию УИС может превратиться в одно из самых технически оснащенных ведомств, что естественно окажет значительную помощь персоналу исправительных учреждений в борьбе с пенитенциарной преступностью.

К.А. Костенко,
заведующий кафедрой уголовного права, криминологии и уголовного процесса Хабаровского филиала Московской академии Следственного комитета Российской Федерации

О практике обеспечения информационной безопасности в системе СК России посредством мониторинга СМИ и информационно-телекоммуникационной сети «Интернет»

Мониторинг СМИ и информационно-телекоммуникационной сети «Интернет» (далее также – мониторинг СМИ и сети «Интернет») является одним из наиболее важных направлений взаимодействия следственных органов СК России со средствами массовой информации. Потребность в нем продиктована необходимостью оперативно реагировать на события и принимать решения в условиях полной информированности.

Необходимо отметить, что в системе СК России защите информации, обеспечению ее безопасности и конфиденциальности уделяется особое внимание. В связи с этим одним из наиболее

[1] Отчет о результатах контрольного мероприятия… С. 219. URL: https://ach.gov.ru/upload/iblock/6c5/6c5a1ce4612053f63eb1805aca2a0e26.pdf

важных аспектов обеспечения информационной безопасности является мониторинг СМИ и сети «Интернет».

Результаты такого мониторинга предоставляют широкие возможности его использования, в том числе и для внесения корректировок по управлению объектом или процессом. «При этом наблюдается рост интереса к мониторингу и понимание его сущности среди руководителей»[1]. Следственный комитет Российской Федерации не является исключением.

В настоящее время технология мониторинга СМИ претерпела значительные изменения. Успешно используются современные системы онлайн-мониторинга. На смену технологиям полнотекстового поиска информации пришли технологии семантического анализа текстового материала, позволяющие интеллектуальным автоматизированным системам в десятки и более раз быстрее решать задачи по работе с текстовыми документами. В числе таких задач классификация текстов по совокупности признаков, поиск ключевых слов, выявление контекстных слов (контекста), аннотирование текста, каталогизация текстов и подбор текстов с заданными свойствами и др.

В условиях получения значительного потока информации и необходимости своевременной ее обработки системам профессионального мониторинга в СК России уделяется большое внимание. В частности, следственные органы для мониторинга СМИ и социальных сетей нацелены на использование в том числе специализированных компьютерных программ.

В следственных органах СК России для обеспечения качественного и своевременного мониторинга СМИ используется программа «RSSOwl» (позволяющая отслеживать в режиме реального времени сообщения, публикуемые на сайтах новостных порталов), а также сайт Mediametrics.ru, на котором отражаются наиболее просматриваемые и актуальные на текущий отрезок времени в социальных сетях и блогах новости.

Акцент на применении автоматизированных систем при осуществлении мониторинга СМИ не исключает так называемый мониторинг в ручном режиме, поскольку качественный анализ текста предполагает оценку таких нюансов, как эмоции, угрозы, характер отношений между объектами.

---

[1] *Рычахина Э.Н.* Мониторинг как общая функция управления: монография. Ухта: УГТУ, 2008. С. 7.

Одной из наиболее важных задач мониторинга является оперативность получения информации. И здесь следует учесть, что в информационно-телекоммуникационной сети «Интернет» информация появляется гораздо быстрее, чем на радио, ТВ и в печатных СМИ. Это связано с тем, что для размещения информации в сети «Интернет» практически не существует барьеров, связанных с необходимостью длительной обработки сообщений и согласования такой информации. Все это в совокупности выводит информационно-телекоммуникационную сеть «Интернет» на первое место среди источников для мониторинга.

В подтверждение растущей глобализации сети «Интернет» и ее воздействия на человека следует согласиться с В.Н. Лопатиным, которым еще более четверти века назад при подготовке в Верховном Совете СССР концепции информационной безопасности были сделаны бесспорные выводы о необходимости нормативного закрепления единой информационной среды (пространства), становившейся тогда и, по сути, ставшей сегодня одним из важнейших государствообразующих признаков, а также об усилении информационной зависимости человека от растущего объема потребляемой информации[1].

Эти и другие выводы, нашедшие подтверждение сегодня, в условиях построения глобального информационного общества, в действительности выводят сеть «Интернет» для мониторинга на первое место среди всего разнообразия средств массовой информации. Так, по итогам 2019 г. более 87% от общего количества сообщений с упоминаниями СК России опубликовано на интернет-ресурсах[2].

Мониторинг СМИ и сети «Интернет» представляет собой определенную систему действий, представляющих собой трудоемкий процесс. Кропотливость и монотонность – характерные черты этой непростой работы. Упустить в потоке информации наиболее важную, свидетельствующую о совершенном преступлении или о вмешательстве в деятельность органа никак нельзя. В связи с этим сотрудниками, ответственными за взаимодействие со СМИ, в ежесуточном режиме осуществляется мониторинг сети

---

[1] *Лопатин В.Н.* Проблемы и перспективы кодификации законодательства в сфере информационного права и интеллектуальной собственности // Информ. право. 2014. № 3. С. 7–8.

[2] Медиалогия: URL: https://www.mlg.ru/ (дата обращения: 10.02.2020).

«Интернет» (Яндекс-новости), RSS-ленты информационных агентств, социальные сети «ВКонтакте», «Фейсбук», Instagram, видеохостинг YouTube, сайт Change.org.

Как правило, первичная информация из нескольких источников достаточна для принятия решения об организации проверки. Между тем в некоторых случаях, например при поиске информации по запросу следователя, при изучении конкретного вопроса или в случае, когда нужно найти, чем закончилась та или иная озвученная в СМИ информация и становилась ли она предметом упоминаний в СМИ, применяется мониторинг СМИ по заданной тематике.

В СК России данные мониторинга СМИ, а также сети «Интернет» используются как для реализации управленческих функций, так и для оперативного и качественного расследования преступлений в соответствии с подследственностью, установленной уголовно-процессуальным законодательством. Выполнение рассматриваемой задачи напрямую связано со своевременным выявлением распространенных в СМИ сведений о совершенных преступлениях и немедленной организацией их предварительного расследования. Это позволяет оперативно приступить к восстановлению нарушенных прав и законных интересов граждан, потерпевших от преступлений.

Необходимо подчеркнуть, что одна из основных функций мониторинга СМИ в системе СК России – это выявление резонансных происшествий, а также ситуаций, затрагивающих права и законные интересы социально незащищенных категорий граждан и требующих реакции правоохранительных органов[1]. Особое внимание уделяется сюжетам и информации о нарушении прав граждан, в особенности детей, инвалидов, ветеранов и других социально незащищенных слоев населения, о чрезвычайных происшествиях и преступлениях, а также об иных вызвавших повышенный общественный резонанс темах.

Наиболее опасны распространенные в СМИ антиобщественные противоправные лозунги, направленные на подрыв

[1] Приказ Председателя СК России от 13.05.2019 № 56 «Об утверждении Инструкции об организации взаимодействия СК России со СМИ, сайтами в информационно-телекоммуникационной сети «Интернет», не являющимися средствами массовой информации, а также с социальными сетями».

национальной безопасности, потребителями которых являются в том числе несовершеннолетние[1].

Статистические данные по мониторингу СМИ и сети «Интернет» свидетельствуют о том, что за последние годы в СК России принципиально изменен подход к организации данной работы. За последние 5 лет (в сравнении с 2015 г.) в 2,6 раза увеличилось число организованных по результатам мониторинга СМИ и сети «Интернет» процессуальных проверок (с 701 до 1874) и на 21% среднее число ежегодно возбуждаемых по итогам их проведения уголовных дел (с 257 до 324)[2].

В целях повышения эффективности мер реагирования на сообщения о готовящихся или совершенных преступлениях, отнесенных к подследственности следователей Следственного комитета Российской Федерации, распространенных в СМИ, а также в информационно-телекоммуникационной сети «Интернет», Председателем СК России 10.05.2017 издано распоряжение № 43/206р «О дополнительных мерах, направленных на повышение эффективности проверки сообщений о преступлениях, распространенных в СМИ».

Таким образом, в числе основных задач мониторинга СМИ и сети «Интернет», обеспечивающих деятельность по защите информации, а также недопущению какой-либо компрометации, можно назвать:

выявление информации о совершенных преступлениях, подследственных СК России, и немедленная организация их предварительного расследования;

осуществление мер по оперативному реагированию на распространяемую в СМИ информацию об общей ситуации в Следственном комитете, следственных органах и организациях Следственного комитета;

своевременное информирование руководителей Следственного комитета, руководителей следственных органов и организаций Следственного комитета о чрезвычайных ситуациях и происшествиях, сведения о которых распространяются в СМИ;

---

[1] *Арефьева Л.В., Магомедов Г.А.* Проблема разжигания национальной и религиозной нетерпимости в современных СМИ // Рос. следователь. 2012. № 19.

[2] Медиалогия: URL: https://www.mlg.ru/ (дата обращения: 10.02.2020).

систематическое и оперативное информирование общественности о деятельности Следственного комитета, способствующее улучшению положительного облика Следственного комитета и его сотрудников в обществе, повышению уровня доверия к Следственному комитету;

своевременное выявление фактов распространения в СМИ недостоверной и ложной информации о деятельности Следственного комитета, его следственных органов и организаций, а также о сотрудниках Следственного комитета в связи с исполнением ими должностных обязанностей;

своевременное предупреждение и выявление фактов коррупции и конфликта интересов на службе; использования служебного положения для оказания влияния на деятельность государственных органов, органов местного самоуправления, организаций, должностных лиц, государственных (муниципальных) служащих и граждан при решении вопросов личного характера; совершение проступков, порочащих честь и достоинство сотрудников СК России.

Подводя итоги, необходимо еще раз подчеркнуть, что «зачастую именно взаимодействие правоохранительных органов со СМИ в современных условиях является мощным фактором в успешном решении задач по борьбе с преступностью»[1] и обеспечению информационной безопасности. При этом проводимый в СК России мониторинг СМИ и сети «Интернет» действительно является важной составляющей процесса обеспечения информационной безопасности СК России, защиты прав и законных интересов граждан и организаций, потерпевших от преступлений.

---

[1] *Костенко К.А.* Роль СМИ в раскрытии преступлений серийных и прошлых лет // Раскрытие и расследование преступлений серийных и прошлых лет: сб. материалов Междунар. науч.-практ. конф. (Москва, 16 марта 2017 г.) / под общ. ред. А.И. Бастрыкина. М.: Моск. акад. СК России, 2017. С. 258–259.

Б.Я. Гаврилов,
профессор кафедры управления
органами расследования
преступлений Академии
управления МВД России, доктор
юридических наук, профессор

Проблемы реализации отдельных положений уголовно-процессуального законодательства в условиях противодействия расследованию преступлений, совершаемых с использованием цифровых технологий

На развитие цивилизации и непосредственно на большинство сфер человеческой деятельности прямое или опосредованное влияние оказывает научно-технический прогресс, в условиях которого и осуществляется деятельность правоохранительных органов по раскрытию и расследованию преступлений, включая уголовно наказуемые деяния, совершаемые с использованием цифровых технологий. Последние реализуются в процессе выполнения объективной стороны таких «классических» сегодня составов преступлений, как незаконный оборот наркотических средств (ст. 228, 228^1 УК РФ), мошенничество с использованием электронных средств платежа (ст.159^3 УК РФ) и др., и формируют необходимость законодательного закрепления новых составов уголовно наказуемых деяний – так называемой киберпреступности.

Определение понятия «информационные технологии» законодателем дано в ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Под ними следует понимать процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Говоря о масштабах преступности с использованием информационно-коммуникационных технологий, следует указать на ее стремительный рост в последние годы. Наглядно это подтверждается статистическими данными ГИАЦ МВД России, со-

гласно которым в 2020 г. в России было зарегистрировано порядка 510,4 тыс. преступлений данного вида, что на 73,4% превышает уровень 2019 г. (294,4 тыс. таких преступлений), а последний, в свою очередь, на 68,5% превышает аналогичный показатель 2018 г. В целом удельный вес деяний данной категории в общем массиве преступлений в 2020 г. составил 25,2% против 4,4% в 2017 г., или возрос почти в 6 раз. Таких темпов прироста как отдельных видов преступлений, так и в целом преступности российская статистика не знала. Опасность состоит и в том, что в истекшем году почти каждое второе из них было тяжким или особо тяжким преступлением.

В условиях трансформации современной преступности[1] особую актуальность приобретают вопросы преодоления противодействия расследованию преступлений, совершенных с использованием цифровых технологий.

Ведя речь о воздействии цифровых технологий на преступную деятельность, следует указать кроме стремительного роста преступности и на ее поступательное развитие ввиду появления новых способов совершения преступлений и интеграции цифровых технологий в имеющиеся способы. Это обусловливает необходимость не только изучения этих способов методами как юридических, так и технических наук, но и развития подходов к изучению цифровых следов и производных от них электронных доказательств, без чего не может обходиться современный процесс расследования преступлений.

Рассматривая эти направления, следует обратиться к работе В.Б. Вехова и С.В. Зуева «Цифровая криминалистика»[2], в которой преступления, связанные с использованием цифровых технологий, авторы разделяют на два типа:

1) преступления, посягающие на цифровую инфраструктуру, работоспособность информационных систем и банков данных и цифровую информацию. В этом случае цифровые технологии

---

[1] *Гаврилин Ю.В.* Тенденции цифровой трансформации преступности и факторы, ее обуславливающие // Стратегическое развитие системы МВД России: состояние, тенденции, перспективы: сб. тр. Междунар. науч.-практ. конф. / под общ. ред. И.Г. Чистобородова, А.Л. Ситковского, В.О. Лапина, 2020.

[2] *Вехов Б.В., Зуев С.В.* Цифровая криминалистика. М.: Юрайт, 2021. С. 295–297.

определяют общие или отдельные характеристики предмета преступного посягательства;

2) преступления, при совершении которых цифровые технологии интегрированы в способ совершения преступления.

К первой группе В.Б. Вехов и С.В. Зуев относят преступления, связанные с использованием вредоносного программного обеспечения: вирусов, троянов, с помощью которых происходит заражение компьютерных устройств. Такие преступления в российском уголовном праве носят название преступлений в сфере компьютерной информации и ответственность за них предусмотрена ст. 272–274[1] УК РФ. Субъекты преступлений в большинстве случаев обладают специальными навыками в области программирования, сетевого администрирования, компьютерной безопасности и т.д.

Необходимо также учитывать, что преступления этой группы способны посягать не только на общественные отношения в сфере компьютерной информации и цифровых технологий, но и на конституционные права человека и гражданина, сферу экономики, здоровья населения и общественной нравственности. Такого рода преступления часто являются трансграничными и латентными.

Вторая группа, как отмечают указанные авторы, включает в себя общеуголовные преступления, при совершении которых использование цифровых технологий является частью способа подготовки, совершения или сокрытия преступления. В этом случае преступники используют мобильные приложения-мессенджеры, подмену номера SIM-карты и другие способы совершения преступлений.

Здесь необходим анализ информации о соединениях между абонентами и(или) абонентскими устройствами, для чего эта деятельность включается в план расследования, а непосредственно анализ SMS-сообщений, сообщений в мессенджерах и социальных сетях необходим для подтверждения факта совершения преступления и выявления роли соучастников противоправного деяния.

При этом следует отметить, что особенностью преступлений обоих типов является то, что в процессе их совершения формируется система цифровых следов, которые могут быть обнаружены,

подвергнуты исследованию, по результатам которого они получают статус доказательств по уголовному делу. Одновременно следует учитывать, что каждое преступление с использованием цифровых технологий имеет самостоятельный механизм следообразования, а в силу этого собственные способы сокрытия. Это обусловливает разнообразие как специальных технических средств, используемых правоохранительными органами, так и средств уголовно-процессуального доказывания таких преступлений.

Говоря о цифровых технологиях, используемых в деятельности правоохранительных органов по преодолению противодействия расследованию преступлений указанного вида, следует указать на необходимость адаптации существующих базовых алгоритмов работы с информацией для решения задач криминалистической деятельности[1].

Для правоприменителей интерес в первую очередь представляют средства по работе с цифровыми следами, включая программные и программно-аппаратные технические средства, направленные на выявление необходимой информации, содержащейся в веб-пространстве, социальной сети, памяти базовой станции сотовой связи, смартфоне и т.д. Обнаружение цифровых следов относится и к работе по преодолению умышленного или случайного противодействия, например, для преодоления защиты смартфона, изъятого у преступника. Для этого могут быть использованы специализированные программные и программно-аппаратные комплексы, такие как Celebrite UFED, XRY, «Мобильный криминалист» и пр.

Средством обнаружения информации могут быть также общедоступные технологии, к примеру, поисковые системы, мобильные приложения (например, getcontact – для определения круга связей лица), сервисы (например, whois – для установления владельца и места физического расположения веб-сайта).

Рассматривая систему мер по преодолению противодействия расследованию преступлений, совершенных с использованием цифровых технологий, следует их разграничить на право-

---

[1] *Рудых А.А.* Информационно-технологическое обеспечение криминалистической деятельности по расследованию преступлений в сфере информационных технологий: дис. … канд. юрид. наук. Ростов н/Д., 2020. С. 61.

вые, включая уголовно-процессуальные, а также организационные и криминалистические. Последние две не входят в предмет рассмотрения настоящей публикации.

В число правовых мер входят:

уголовно-процессуальные средства преодоления противодействия расследованию преступлений, к которым относятся процессуальные правила формирования доказательств на электронных носителях информации:

а) ст. 164^1 УПК РФ, регулирующая основания для изъятия электронных носителей информации и устанавливающая требования обязательного участия при этом специалиста;

б) ч. 7. ст. 185 УПК РФ – о правилах осмотра и выемки электронных сообщений;

в) п. 5 ч. 2 ст. 82 УПК РФ, устанавливающий основания и порядок хранения вещественных доказательств в качестве электронных носителей информации и др.;

нормы федерального законодательства:

а) ст. 10^1 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», возлагающая на интернет-провайдеров обязанности по идентификации пользователей и хранению на территории Российской Федерации передаваемого пользователями контента и фактов доступа к информационным ресурсам;

б) ст. 44, 64 Федерального закона от 07.07.2003 № 126-ФЗ «О связи», положениями которых на оператора связи возложены аналогичные обязанности;

в) Федеральный закон от 29.07.2017 № 241-ФЗ, нормы которого обязывают организатора обмена мгновенными сообщениями (мессенджеров) обеспечивать идентификацию своих клиентов;

г) положение Банка России от 09.06.2012 № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств», устанавливающее перечень сведений, подлежащих фиксации оператором электронных платежных средств, и др.

Повысить эффективность деятельности органов предварительного следствия по преодолению противодействия расследо-

ванию преступлений, совершенных с использованием цифровых технологий, призвана и введенная в эксплуатацию в 2019 г. информационная система «Дистанционное мошенничество»[1], которая аккумулирует данные об использованных при совершении преступления идентификационных данных средств связи, номерах банковских карт и банковских счетов, номерах документов, удостоверяющих личность, а также реквизитах организаций, упоминающихся в материалах дела.

В заключение следует указать, что проблема преодоления противодействия расследованию преступлений, совершаемых с использованием цифровых технологий, является одной из наиболее острых в деятельности правоохранительных органов.

Ю.В. Гаврилин,
начальник кафедры
управления органами
расследования преступлений
Академии управления
МВД России, доктор
юридических наук, доцент

Научные основы преодоления противодействия расследованию преступлений, совершенных с использованием информационно-коммуникационных технологий

Основоположниками современного учения о противодействии расследованию преступлений и мерах по его преодолению являются В.Н. Карагодин[2] и С.Ю. Журавлев[3]. Оба автора определяют противодействие расследованию как умышленные действия (систему действий), направленные на воспрепятствование

[1] Приказ МВД России от 22.04.2020 «О вводе в эксплуатацию подсистемы «Дистанционное мошенничество» ПТК ИБД-Ф».
[2] *Карагодин В.Н.* Преодоление противодействия предварительному расследованию. Свердловск, 1992.
[3] *Журавлев С.Ю.* Противодействие деятельности по раскрытию и расследованию преступлений и тактика его преодоления: дис. ... канд. юрид. наук. Н. Новгород, 1992.

выполнению задач расследования и установлению объективной истины по уголовному делу. В разные годы проблемам противодействия расследованию преступлений посвятили свои труды Р.С. Белкин, А.Ф. Волынский, В.П. Лавров, а также их многочисленные последователи. В практически неизменном виде данное определение существует и в современных работах различных авторов[1].

Сегодня имеются все основания констатировать, что вопросы преодоления противодействия расследованию сложились в хорошо проработанную частную криминалистическую теорию, носящую сквозной характер, поскольку она затрагивает все без исключения разделы науки криминалистики.

В условиях цифровой трансформации современной преступности[2] особую актуальность приобретают вопросы преодоления противодействия расследованию преступлений, совершенных с использованием информационно-коммуникационных технологий[3].

---

[1] *Бабаева Э.У.* Некоторые теоретические и практические аспекты учения о преодолении противодействия уголовному преследованию. М., 2004; *Гармаев Ю.П.* Преодоление противодействия уголовному преследованию в следственных изоляторах: монография. М.: Юрлитинформ, 2019; *Косынкин А.А.* Преодоление противодействия расследованию преступлений в сфере компьютерной информации: монография / под ред. Н.А. Подольного. М.: Юрлитинформ, 2013; *Противодействие* расследованию преступлений и меры по его преодолению: учеб. пособие / под общ. ред. Б.Я. Гаврилова, В.П. Лаврова; М.: Акад. управления МВД России, 2014; *Рахматуллин Р.Р.* Противодействие раскрытию и расследованию преступлений: теория и практика упреждения, выявления и преодоления: монография. М.: Юрлитинформ, 2018 и др.

[2] *Гаврилин Ю.В.* Тенденции цифровой трансформации преступности и факторы, ее обуславливающие // Стратегическое развитие системы МВД России: состояние, тенденции, перспективы: сб. тр. Междунар. науч.-практ. конф. / под общ. ред. И.Г. Чистобородова, А.Л. Ситковского, В.О. Лапина. М., 2020.

[3] По данным ГИАЦ МВД России, в 2019 г. в России зарегистрировано 294 409 преступлений, совершенных с использованием информационно-коммуникационных технологий, что на 68,5% превышает аналогичный показатель 2018 г. Удельный вес деяний данной категории в общем массиве преступлений составил 14,5% (2018 г. – 8,8%, 2017 г. – 4,4%). При этом около половины (48,5%) из них относятся к тяжким и особо тяжким преступлениям (142 728, +149%), каждое второе (53,3%) совершено с использованием сети «Интернет» (157 036, +45,4%), почти 40% с использованием средств мобильной связи (116 154, +89,5%). В общем массиве зарегистрированных деяний указанной категории преобладают мошенничества (136 709, или 46,4%) и кражи (98 798, или 33,6%). Их количество возросло на 42,6 и 202,4% соответственно. См.: Официальный сайт МВД России. URL: https://xn--b1aew.xn--p1ai/Deljatelnost/statistics

В большинстве случаев информационно-коммуникационные технологии применяются при совершении преступлений против личности (путем нарушения неприкосновенности частной жизни, доведения до самоубийства, нарушения авторских прав), собственности (путем кражи, мошенничества, вымогательства), в сфере незаконного оборота наркотических средств и психотропных веществ, а также преступлений экстремистской направленности. В качестве одной из мер борьбы с этими видами преступлений в уголовное законодательство введен ряд специальных составов, призванных обеспечить защиту информационной сферы от противоправных посягательств, в частности: мошенничество с использованием электронных средств платежа (ст. 159^3 УК РФ), мошенничество в сфере компьютерной информации (ст. 159^6), преступления в сфере компьютерной информации (гл. 28 УК РФ). Кроме того, такой квалифицирующий признак, как использование при совершении преступления информационно-телекоммуникационных сетей, включая сеть «Интернет», включен законодателем в диспозиции 19 норм уголовного закона.

Основными способами противодействия расследованию обозначенных преступлений являются:

использование программ-ремейлеров, обеспечивающих переадресацию отправлений электронной почты и подмену информации об электронном адресе отправителя электронным адресом ремейлера или иным подменным адресом. В результате получатель электронного почтового отправления лишается возможности установить личность отправителя. Ремейлеры обеспечивают возможность реализации так называемых фишинговых схем (от англ. to fish – ловить рыбу), основанных на рассылке электронных писем якобы от имени государственных и муниципальных органов, судов, банков, иных организаций, вызывающих доверие у потерпевшего. После открытия такого письма в информационную систему потерпевшего попадает вредоносное программное обеспечение, позволяющее втайне от него выполнять несогласованные функции: собирать и передавать злоумышленникам персональные данные (включая платежную информацию), производить блокирование системы с требованием платы за разблокировку. Использование ремейлеров при этом существенно затрудняет установление лица, совершившего преступление.

использование программ-анонимайзеров, обеспечивающих подмену используемого абонентом сети «Интернет» уникального IP-адреса, предоставленного ему провайдером при подключении к сети. При этом происходит замена IP-адреса пользователя на IP-адрес программы-анонимайзера, а также подмена информации об используемом сетевом браузере, параметрах его настройки, удаление запросов и ответов веб-сервера от служебных cookie-файлов, используемых для формирования истории посещения определенных интернет-ресурсов пользователем сети. Анонимайзеры позволяют обходить ограничения на доступ к информационным ресурсам, содержащим информацию, распространение которой в Российской Федерации запрещено.

Большинство анонимайзеров просты в использовании: в поисковую строку вводится сетевой адрес ресурса, доступ к которому требуется осуществить не с IP-адреса пользователя, а с IP-адреса анонимайзера, расположенного, как правило, за рубежом.

Особой разновидностью анонимайзеров являются VPN-сервисы (от англ. virtual private network – виртуальная частная сеть). Они обеспечивают создание защищенного информационного канала (туннеля) между устройством, с которого осуществляется вход в сеть «Интернет», и сервером, обеспечивающим работу VPN-сервиса, расположенным, как правило, за рубежом, осуществляя переадресацию сообщений. В отличие от обычных анонимайзеров VPN-сервисы осуществляют шифрование данных, отправляемых или получаемых с их использованием.

Для целей обеспечения более надежного сокрытия данных, позволяющих идентифицировать лицо, осуществившее вход в сеть «Интернет», VPN-сервисы нередко используются совместно с прокси-серверами – физическими устройствами или специальными программами, обеспечивающими роль посредника между подключаемым к сети «Интернет» устройством и самой сетью. Учитывая, что к одному прокси-серверу могут подключаться сотни различных устройств, все они для внешних пользователей будут иметь общий IP-адрес – адрес прокси-сервера;

использование TOR-браузеров – программ, обеспечивающих возможность выхода в анонимную сеть TOR (от англ. *the onion router* – луковичная маршрутизация). Анонимность в сети TOR реализуется с помощью разбиения каждого сетевого запроса

на множество небольших фрагментов и их пересылки от отправителя к получателю через разные маршрутизаторы. Именно в данном сегменте сети, не индексируемом традиционными поисковыми средствами (Яндекс, Google), размещается абсолютное большинство виртуальных торговых площадок по нелегальной продаже запрещенных к свободному обороту объектов (оружие, боеприпасы, наркотики и пр.). С указанной целью сети TOR создаются специализированные сайты, физически размещенные на серверах вне юрисдикции Российской Федерации, предлагающие приобрести запрещенные к обороту объекты и позволяющие производить оплату. Функционально данные информационные ресурсы представляют собой интернет-магазины, реализующие криминальные товары и предлагающие незаконные услуги. После проведения оплаты покупателю сообщаются геокоординаты и высылается фотоизображение места закладки – тайника, в котором находится заранее размещенный в нем объект криминальной сделки.

Система мер, направленных на преодоление противодействия расследованию преступлений, совершенных с использованием информационно-коммуникационных технологий, включает в себя правовые, организационные и криминалистические меры.

В число правовых мер входит в первую очередь комплекс положений действующего законодательства, направленных на деанонимизацию пользователей информационных ресурсов сети «Интернет», а именно:

ст. 10^1 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», возлагающая на интернет-провайдеров обязанности по идентификации пользователей и хранению на территории Российской Федерации передаваемого пользователями контента и фактов доступа к информационным ресурсам;

ст. 44, 64 Федерального закона от 07.07.2003 № 126-ФЗ «О связи», которыми на оператора связи возложены аналогичные обязанности;

Федеральный закон от 05.05.2014 № 110-ФЗ, предусматривающий ограничения для анонимных платежей, совершаемых онлайн, и процедуру обязательной идентификации пользователей электронных средств платежа;

Федеральный закон от 29.07.2017 № 241-ФЗ, обязывающий организатора обмена мгновенными сообщениями (мессенджеров) обеспечивать идентификацию своих клиентов;

положение Банка России от 09.06.2012 № 382-П, устанавливающее перечень сведений, подлежащих фиксации оператором электронных платежных средств.

Во-вторых, к числу правовых средств преодоления противодействия расследованию рассматриваемых преступлений относятся нормы, регламентирующие порядок формирования доказательств на электронных носителях информации, а именно:

п. 5 ч. 2 ст. 82 УПК РФ, устанавливающий основания и порядок хранения электронных носителей информации – вещественных доказательств;

ст. 164^1 УПК РФ, устанавливающая основания для изъятия электронных носителей информации, допускающая копирование информации и вводящая требование обязательного участия при этом специалиста;

ч. 7 ст. 185, позволяющая производить осмотр и выемку электронных сообщений и др.

К организационным мерам преодоления противодействия расследованию рассматриваемых преступлений относятся:

закрепление специализации следователей на расследовании преступлений в сфере информационных технологий, с учетом опыта и наличия специальных познаний в указанной области;

заблаговременное обсуждение материалов проверок сообщений о преступлениях в аппаратах следственных органов МВД России по субъектам Российской Федерации с уделением особого внимания их полноте и качеству, проведению необходимых исследований, результатам оперативно-розыскных мероприятий;

использование территориальными органами внутренних дел систем электронного документооборота, а также заключение соглашений об информационном обмене с кредитно-финансовыми организациями, операторами платежных систем, операторами связи и интернет-провайдерами, что позволяет с миниальными временными затратами получать необходимые сведения об анкетных данных абонента по номерам телефона и СИМ-карты, о подключенных услугах и произведенных платежах, а также о движении денежных средств клиента кредитно-финансовой орга-

низации, включая данные об отправителе, получателе, сумме операции, дате и времени ее проведения, наименовании сервиса, через который она была проведена, IP-адресе, с которого произведена транзакция, IMEI-номере абонентского устройства, при получении наличных через банкомат – его номер, место установки, видеозапись встроенной камеры наблюдения и другие сведения, имеющие значение для полного, всестороннего и объективного производства расследования в разумные сроки.

В числе криминалистических средств преодоления противодействия расследованию преступлений, совершенных с использованием информационно-коммуникационных технологий, следует выделить в первую очередь обоснованные Г.З. Гаспаряном[1] тактические приемы производства следственных действий, направленных на получение невербальной доказательственной информации, в частности:

1) радиоподавление, направленное на недопущение приема/передачи информации, подачу команд с использованием беспроводных компьютерных сетей и сетей мобильной связи;

2) преодоление аппаратно-программного шифрования данных, состоящее в использовании технико-криминалистических средств получения доступа к информации, находящейся на электронном носителе, защищенной алгоритмом шифрования;

3) нелинейная локация, направленная на обнаружение и определение местонахождения устройств, содержащих электронные компоненты во включенном и в выключенном состоянии;

4) криминалистический анализ данных, состоящий в систематизации содержащейся на электронном носителе информации, позволяющей выполнять поиск данных с заданными характеристиками;

5) криминалистическое копирование данных, позволяющее создавать их дубликат, соответствующий оригиналу как по содержанию, так и по технологическим свойствам;

6) формирование по особым алгоритмам контрольных сумм изымаемой в процессе следственного действия информации, обеспечивающее достоверность доказательств на основе сопо-

[1] См.: *Гаспарян Г.З.* Расследование хищений денежных средств, совершенных с использованием информационных банковских технологий: автореф. дис. … канд. юрид. наук. М., 2020. С. 26–27.

ставления параметров изъятой и впоследствии исследуемой информации;

7) изготовление скриншотов в процессе фиксации доказательственной информации, состоящее в копировании содержания экрана с использованием встроенной функции операционной системы;

8) гибернация, состоящая в переводе изымаемого устройства в энергосберегающий режим, позволяющий сохранить содержание оперативной памяти.

Кроме того, повысить уровень информационно-аналитического обеспечения органов предварительного следствия в процессе расследования преступлений, совершенных с использованием информационно-коммуникационных технологий, призвана введенная в эксплуатацию в 2019 г. информационная система «Дистанционное мошенничество»[1], предназначенная для сбора, систематизации, обработки и анализа сведений, устанавливаемых в рамках расследования уголовных дел о преступлениях, совершенных дистанционным способом. Система аккумулирует данные об использованных при совершении преступления идентификационных данных средств связи, номерах банковских карт и банковских счетов, номерах документов, удостоверяющих личность, а также реквизитах организаций, упоминающихся в материалах дела.

К числу криминалистических средств преодоления противодействия расследованию рассматриваемых преступлений следует отнести и использование cookie-файлов для установления лица, совершившего преступление. Cookie-файл представляет собой массив данных, который интернет-сайт передает в браузер пользователя и собирает о нем. Получаются посредством запроса администратору интернет-ресурса, использованного при совершении преступления. Позволяют преодолевать попытки анонимизации путем использования VPN, TOR, SSL, программ-анонимайзеров; идентифицировать лицо, несмотря на предпринимаемые меры подмены IP-адреса; установить факт использования одного компьютера при обращении к нескольким сайтам

[1] Приказ МВД России от 22.04.2020 «О вводе в эксплуатацию подсистемы «Дистанционное мошенничество» ПТК ИБД-Ф».

(например, Авто); получить сведения по всем публикациям, размещенным определенным лицом.

В заключение следует отметить, что приведенный перечень не является исчерпывающим, постоянно расширяется и адаптируется к новым способам и вызовам современной преступности.

Д.И. Ережипалиев,
заведующий отделом
НИИ Университета прокуратуры
Российской Федерации,
кандидат юридических наук

Региональные подходы к обеспечению информационной безопасности детей

В контексте цифровых технологий в борьбе с преступностью значительный интерес представляют региональные подходы к проблеме обеспечения информационной безопасности, особенно несовершеннолетних.

В большинстве субъектов Российской Федерации вопросы обеспечения информационной безопасности детей в настоящее время регулируются региональными законами, направленными либо на охрану прав ребенка в целом (республики Башкортостан и Дагестан, Кабардино-Балкарская Республика, Краснодарский и Ставропольский края, Белгородская, Новосибирская, Пензенская, Свердловская, Томская, Тульская, Челябинская области и др.), либо на предупреждение причинения вреда здоровью детей, их физическому, интеллектуальному, психическому, духовному и нравственному развитию (республики Бурятия, Ингушетия, Карелия и Татарстан, Камчатский край, Санкт-Петербург, Амурская, Брянская, Иркутская, Калужская, Курганская, Ленинградская, Магаданская, Новгородская, Омская, Оренбургская, Ростовская, Сахалинская, Тамбовская области).

Значительный импульс развитию указанных законов дало принятие Федерального закона от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и раз-

витию» (далее – Федеральный закон от 29.12.2010 № 436-ФЗ), после вступления в силу которого многие региональные законы в области охраны прав ребенка были дополнены положениями, направленными на защиту ребенка от информации, пропаганды и агитации, наносящих вред его здоровью, нравственному и духовному развитию, а в ряде субъектов Российской Федерации были приняты соответствующие новые законы. В отдельных регионах вопросы обеспечения информационной безопасности детей нашли отражение в законах субъектов Российской Федерации еще до принятия Федерального закона от 29.12.2010 № 436-ФЗ (в Брянской, Калининградской, Курганской и Свердловской областях и др.), что свидетельствует о попытке региональных законодателей в рамках полномочий субъектов Российской Федерации законодательно закрепить вопросы обеспечения информационной безопасности детей, которые при отсутствии федерального законодательства все же приобретали очертания самостоятельного правового института, требующего правовой регламентации.

Как показал анализ, большинство региональных законов содержат специальные нормы, направленные на обеспечение информационной безопасности детей. Как правило, органы государственной власти субъекта Российской Федерации, закрепляя такие нормы, предусматривают свое участие в осуществлении мер по защите ребенка от информации, пропаганды и агитации, наносящих вред его здоровью, нравственному и духовному развитию, в том числе от национальной, классовой, социальной нетерпимости, от рекламы алкогольной продукции и табачных изделий, от пропаганды социального, расового, национального и религиозного неравенства, от информации порнографического характера, от информации, пропагандирующей нетрадиционные сексуальные отношения, а также от распространения печатной продукции, аудио- и видеопродукции, пропагандирующей насилие и жестокость, наркоманию, токсикоманию, антиобщественное поведение, от информации, склоняющей несовершеннолетних к суицидальным действиям.

Кроме того, подобные нормы предусматривают, что в целях защиты детей от информации, причиняющей вред их здоровью и (или) развитию, Федеральным законом от 29.12.2010 № 436-ФЗ

устанавливаются требования к распространению среди детей информации, в том числе требования к осуществлению классификации информационной продукции, ее экспертизы, государственного надзора и контроля за соблюдением законодательства Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию. В целях обеспечения безопасности жизни, охраны здоровья, нравственности ребенка, защиты его от негативных воздействий в порядке, определенном уполномоченным Правительством Российской Федерации федеральным органом исполнительной власти, проводится экспертиза (социальная, психологическая, педагогическая, санитарная) настольных, компьютерных и иных игр, игрушек и игровых сооружений для детей.

В отдельных субъектах Российской Федерации региональные законы таких специальных норм не содержат, а их положения в части обеспечения информационной безопасности детей носят фрагментарный характер (в Камчатском крае, Белгородской, Калужской, Новгородской, Омской, Оренбургской, Ростовской, Сахалинской, Пензенской и Челябинской областях и др.).

Как правило, в таких законах содержатся следующие положения:

распространение информации, доступ детей к которой запрещен или ограничен в соответствии с Федеральным законом от 29.12.2010 № 436-ФЗ;

не допускается нахождение детей (лиц, не достигших возраста 18 лет) без сопровождения родителей (лиц, их заменяющих) или лиц, осуществляющих мероприятия с участием детей, в ночное время (с 22 часов до 6 часов) на объектах (на территориях, в помещениях) юридических лиц или граждан, осуществляющих предпринимательскую деятельность без образования юридического лица, которые предназначены для обеспечения доступа к информационно-телекоммуникационной сети «Интернет»;

деятельность организаций различных форм собственности, общественных и иных организаций, а также граждан, осуществляющих предпринимательскую деятельность без образования юридического лица, должна соответствовать основным требованиям, установленным законами и иными нормативными право-

выми актами Российской Федерации и Челябинской области в части определения порядка, условий и качества предоставляемых услуг и (или) товаров в целях охраны здоровья детей, и должна быть направлена на защиту детей от рекламы алкогольной продукции и табачных изделий, распространения печатной продукции, аудио- и видеопродукции, пропагандирующей насилие и жестокость, порнографию, наркоманию, токсикоманию, антиобщественное поведение, а также иной продукции и информации, негативно влияющей на физическое, интеллектуальное, психическое, духовное и нравственное развитие детей.

Анализ региональных законов свидетельствует, что нормы, содержащиеся в них, зачастую носят общий, декларативный характер и во многом дублируют положения федерального законодательства, что еще раз подтверждает необходимость четкого разграничения полномочий федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации в области обеспечения информационной безопасности детей.

В настоящее время помимо законов субъектов Российской Федерации практически повсеместно разработаны, приняты и реализованы региональные стратегии действий в интересах детей, в которых предусмотрены в том числе мероприятия по обеспечению информационной безопасности детей, утверждены планы первоочередных мероприятий по реализации этих стратегий, созданы и действуют координационные советы по их реализации; приняты и действуют региональные концепции, в том числе направленные на обеспечение информационной безопасности детей; утверждены планы мероприятий по обеспечению информационной безопасности детей, производства и оборота информационной продукции для детей; в отдельных регионах разработаны и действуют специальные региональные программы по обеспечению информационной безопасности детей.

Определенный интерес представляет опыт Республики Марий Эл. В названном регионе образована и функционирует Межведомственная комиссия при Правительстве Республики Марий Эл по информационной безопасности детей, которая является координационным органом, образованным для взаимодействия тер-

риториальных органов федеральных органов исполнительной власти, органов исполнительной власти Республики Марий Эл, органов местного самоуправления в Республике Марий Эл, общественных объединений, религиозных организаций и иных организаций, индивидуальных предпринимателей и граждан по обеспечению защиты детей от информации, наносящей вред их здоровью и (или) психическому, физическому, духовному и нравственному развитию.

Указанная комиссия в целях реализации возложенных на нее задач выявляет и анализирует причины и условия, способствующие нарушениям требований законодательства Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию, определяет меры по устранению указанных причин и условий; взаимодействует с общественными объединениями, религиозными организациями, иными организациями независимо от их организационно-правовых форм и форм собственности, осуществляющими свою деятельность на территории Республики Марий Эл, и гражданами по вопросам защиты детей от информации, наносящей вред их здоровью и (или) развитию; взаимодействует с территориальными органами федеральных органов исполнительной власти, органами исполнительной власти Республики Марий Эл, органами местного самоуправления по вопросам защиты детей от информации, наносящей вред их здоровью и (или) развитию, и оказывает им организационно-методическую помощь; обобщает и распространяет положительный опыт работы территориальных органов федеральных органов исполнительной власти, органов исполнительной власти Республики Марий Эл, органов местного самоуправления в указанной сфере.

Вместе с тем следует отметить, что не во всех регионах уделяется должное внимание вопросам информационной безопасности детей, несмотря на то что в стратегиях действий в интересах детей большинства субъектов Российской Федерации отмечается сложная обстановка в области распространения информации, представляющей опасность для детей. При этом действие региональных стратегий ограничивалось периодом, аналогичным Стратегии действий в интересах детей на 2012–2017 годы.

На отсутствие должного внимание к данным вопросам указывает то обстоятельство, что далеко не во всех регионах страны приняты соответствующие специальные региональные программы.

В настоящее время проблемы, связанные с обеспечением информационной безопасности детей, нашли отражение в региональных программах в Чувашской Республике, Забайкальском крае, Владимирской, Кировской областях, Кемеровской области – Кузбассе, Нижегородской, Новгородской, Пензенской, Ростовской, Свердловской, Тульской и Ярославской областях, а также в Еврейской автономной области.

Исследование показало, что в субъектах Российской Федерации отсутствует единообразный подход к законодательному регулированию вопросов обеспечения информационной безопасности детей. Зачастую законодательные положения в указанной сфере носят общий, декларативный характер и во многом дублируют положения федерального законодательства, что в определенной степени объясняется отсутствием четкой регламентации в федеральных законах от 06.10.1999 № 184-ФЗ «Об общих принципах организации законодательных (представительных) и исполнительных органов государственной власти субъектов Российской Федерации» и от 29.12.2010 № 436-ФЗ вопроса о разграничении полномочий федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации в области обеспечения информационной безопасности детей в различных сферах оборота информационной продукции, что в свою очередь обусловливает необходимость дальнейшего совершенствования законодательства в указанной сфере.

М.Б. Колбая,
доцент кафедры уголовно-правовых дисциплин Сочинского филиала Всероссийского государственного университета юстиции (РПА Минюста России), кандидат юридических наук

Цифровые технологии как инструмент предупреждения насильственных преступлений, совершаемых на территории Республики Абхазия

Предупреждение насильственных преступлений в Республике Абхазия является важнейшей составной частью деятельности государства. В зависимости от результата этой деятельности можно судить о полноте и качестве выполнения государством своих функций. Что может быть важнее сегодня для Республики Абхазия как государства, перенесшего войну и потерявшего тысячи граждан, чем сохранение их жизни путем повышения эффективности деятельности правоохранительных органов по профилактике насильственной преступности, в том числе и с использованием цифровых технологий.

В связи с этим в первую очередь встает вопрос дальнейшего совершенствования структуры правоохранительных органов, углубления их специализации и повышения уровня квалификации кадров. Важной задачей является обеспечение предупредительной деятельности, которое будет проявляться в развитии единого информационно-аналитического, программного и координационного центра.

Прежде чем приступить к освещению аспектов, связанных с цифровыми технологиями, необходимо кратко изложить и проанализировать ситуацию в сфере борьбы с насильственной преступностью, имеющую место в настоящее время в Абхазии.

Система борьбы с насильственными преступлениями за годы реформ в послевоенный период оказалась разрушенной, разруха и хаос, царившие в послевоенный период, не могли создать благоприятной обстановки для формирования новой адаптиро-

ванной системы предупреждения насильственных преступлений. Лишь начиная с 2001 г. в Абхазии наблюдаются некоторые попытки восстановления системы предупреждения насильственных преступлений.

В связи с военными действиями, развернутыми на территории Республики Абхазия в 1992 г., была разрушена эффективная система профилактики убийств, что привело к увеличению их количества.

А уже в период 1994–2008 гг. в ходе проведенного обобщения по делам об убийствах, совершенных на территории Республики Абхазия, отмечалось снижение количества насильственных преступлений. В 2008–2020 гг. наблюдается относительно стабильная динамика количества убийств с ухудшением качественных характеристик.

Несмотря на позитивные тенденции динамики количественных показателей убийств, наблюдающиеся в Республике Абхазия в последние годы, произошло, как было отмечено, ухудшение качественных характеристик преступлений данного вида, о чем свидетельствует показатель интенсивности убийств в Республике Абхазия (3,4), который вдвое выше, чем в Российской Федерации (1,9). Это является негативным фактором, отрицательно сказывающимся на качественных характеристиках убийств в Республике Абхазия.

Также было выявлено, что в Республике Абхазия увеличивается доля организованных преступлений. Количество организованных убийств, совершаемых в Республике Абхазия, составляет 5% от общего числа убийств, тогда как в Российской Федерации – 1%.

Среди лиц, которые совершают убийства, возрастает доля злостных преступников специфической направленности. В их противоправном поведении начинают просматриваться признаки криминального профессионализма.

Следует отметить, что в Республике Абхазия значительное число убийств совершено по политическим мотивам, а также связано с убийством лиц, деятельность которых заключается в противодействии борьбе с преступностью. Увеличивается доля заказных убийств.

Специфика причин убийств в Республике Абхазия связана с особой политической ситуацией в государстве. С одной стороны, как позитивный факт следует отметить достижение государством независимости, с другой – необходимо учесть отрицательное влияние послевоенного периода, нахождение Республики Абхазия долгие годы в кризисе, повлиявшее на формирование причин убийств и личности убийц.

Необходимо также остановиться на том, что 90% всех убийств совершено с применением незаконно хранящегося оружия и оружия, хранящегося ненадлежащим способом. Таким образом, убийце не составляет особого труда приобрести оружие, ранее нигде не фигурировавшее.

Также следует обратить внимание на то, что в состоянии внезапно возникшей ссоры либо сильного душевного волнения убийца легко может воспользоваться оружием для совершения преступления. Учитывая местный менталитет и поствоенный синдром, данные факты приобретают особую частоту.

Это прослеживается и в некоторых особенностях личности убийц в Республике Абхазия: высокий удельный вес (45%) составляют лица, участвовавшие в военных действиях 1992–1993 гг.

Более высокой, чем в Российской Федерации, является и доля лиц, употребляющих наркотические средства (37%).

Все эти факторы должны учитываться при разработке мер по предупреждению убийств в Республике Абхазия, в том числе и при использовании цифровых технологий.

Очевидно, что при отсутствии постоянного анализа динамики убийств, в том числе их основных причин, правоохранительным органам, в частности органам внутренних дел, невозможно говорить о построении эффективной профилактической системы борьбы с убийствами, а также о выработке стратегии и тактики в данном направлении. По этой причине мы выступаем с предложением обратиться к опыту российских коллег.

Для решения проблемы, связанной с использованием при совершении убийства незаконно хранящегося оружия, необходимо усилить и наладить должный учет и контроль за оружием, хранящимся у населения; наладить выкуп оружия у населения за вознаграждение; определить порядок и систему хранения оружия

с использованием сейфов и специальных ячеек, шкафов, предусмотреть четкую регистрацию лиц, которые ранее совершали убийства. Для осуществления этих мер необходимы разработка и внедрение соответствующей компьютерной базы с использованием цифровых технологий.

Основные предложения по введению цифровых технологий в борьбу с преступностью:

а) осуществить государственный заказ на научные разработки в сфере предупреждения насильственных преступлений и убийств, в частности на базе прогноза развития ситуации и учета обозначившихся потребностей практики;

б) создать организационную базу для экспериментальной проверки научных разработок и процессов их внедрения в практику профилактической работы;

в) создать современную информационную базу с использованием последних достижений компьютерной техники, обеспечивающую мониторинг ситуации, ее прогноз в сопоставлении с состоянием предупредительной деятельности.

На основании индивидуальной профилактики, которая включает выявление характерных объективных и субъективных признаков личности убийцы, определить и внедрить следующие аспекты.

Так как к характерным субъективным признакам относятся склонность к вспышкам гнева, озлобленность, мстительность, дерзость, пьянство и наркомания, а к объективным факторам – систематическое пьянство и потребление наркотиков, судимость за убийства, приобретение, хранение огнестрельного оружия, мелкое хулиганство, учет каждого из этих факторов важен для прогнозирования возможности совершения убийств конкретными лицами и определения методов их индивидуальной профилактики.

Считаем необходимым для качественной предупредительной деятельности организовать выявление всех профессиональных убийц и установить за ними постоянный контроль. Все профессиональные преступники, в первую очередь профессиональные убийцы, должны находиться на учете, а их преступная деятельность отслеживаться безусловно не без помощи новейших

цифровых технологий (камеры слежения, информационно-аналитические базы, сбор и анализ информации о преступниках).

С этой целью необходимо создать в масштабах Республики Абхазия компьютерную базу данных всех профессиональных убийц. Эти данные должны собираться, начиная с участковых инспекторов милиции вплоть до начальников отрядов в исправительных учреждениях. База должна включать также способ совершения убийств, их окружение и любую другую интересующую информацию.

Предложенные меры по созданию базы лиц, совершивших убийства на территории Республики Абхазия, связаны с тяжелой криминогенной ситуацией в регионе и по этой причине требуют незамедлительного внедрения. В процессе изучения материалов уголовных дел за 2015–2020 гг.[1] было выявлено распространение заказных убийств, что свидетельствует о существовании организованного рынка соответствующих услуг в Республике Абхазия.

Борьба с убийствами может быть эффективной только в том случае, если она осуществляется на прочной правовой основе и подкреплена соответствующим технологическим обеспечением. Развитие законодательства Республики Абхазия, нацеленного на профилактику убийств, должно учитывать современные условия существования общества, состояние общественного правосознания и реалии современного мира, основанного на использовании цифровых технологий.

[1] Информационный центр МВД РА, 2020.

Е.В. Демидова-Петрова,
доцент кафедры криминологии
и уголовно-исполнительного
права Казанского юридического
института МВД России,
кандидат юридических наук,
доцент

Возможности Big Data в области предупреждения преступности несовершеннолетних

Сегодня одним из важнейших ресурсов является информация. Реализация информационного ресурса абсолютно во всех сферах деятельности человека дает возможность достичь новых значительных высот. Так, информационный пласт стал настолько велик, что систематизировать, обрабатывать, хранить информацию сформировавшимися, традиционными способами становится сложно.

Термин «Big Data» впервые озвучил редактор журнала Nature Клиффорд Линч еще в 2008 г. В своем труде он говорил о динамичном росте объемов информации, а также утверждал, что освоить в полном объеме весь массив мировой информации будет возможно исключительно благодаря новым инструментам и наиболее развитым технологиям.

Термин «Big Data» (буквальный перевод – большие данные) приобрел широкую популярность. С одной стороны, подобная технология вызывает скептическое отношение, а с другой – значительное количество крупных компаний начали использовать возможности Big Data в своей деятельности.

Еще Н. Марц и Д. Уоррен, исследуя возможности, заложенные в Big Data, говорили о том, что Big Data представляют собой определенные подходы, которые заложены в инструментах, методах анализа, обработки значительных, многообразных объемов информационных данных, которые являются как структурированными, так и неструктурированными. Авторы также указали, что в современных условиях постоянного увеличения количества информации подобные технологии должны быть широко приме-

нимы в целях «распределения информации по многочисленным узлам вычислительной сети»[1].

Так, современный мир изменился. Его основным отличием является возникновение нового онлайн-пространства. Рождение онлайн-пространства повлекло за собой появление новой социальной среды – онлайн социальной среды. В данном контексте следует особое внимание уделить тому, что в онлайн социальной среде представлены и лица несовершеннолетнего возраста.

Одной из значительных особенностей XXI в. является информационная глобализация – социально-технологическое явление, изменившее мир. При этом онлайн социальная среда представляет собой мир, созданный исходя из возможностей научно-технического прогресса. Термин «онлайн» указывает на «состояние подключения к сети «Интернет». В современном мире становятся очевидными перенос реально существующих связей, изменение, трансформация ранее существовавших и расширение онлайн сетевых коммуникаций.

Итак, в условиях современных реалий и возникновения криминогенных факторов, оказывающих влияние на несовершеннолетних, не позволяющих предвидеть характер возникновения противоправных, преступных явлений, субъектами которых они становятся, появляется потребность в создании системы криминологического учета поведенческих, социальных, экономических, политических, духовных потребностей несовершеннолетних. В новых информационно-коммуникационных технологиях, а именно в Big Data, находятся обсуждаемые возможности. Так, благодаря Big Data становится возможным:

вести мониторинг, учет сайтов, притягивающих внимание лиц несовершеннолетнего возраста;

осуществлять контроль за потребительскими расходами;

выявлять территории, зоны досуга и отдыха;

устанавливать частоту посещения лицами несовершеннолетнего возраста общественных мест;

---

[1] См. подробнее: *Марц Н.* Большие данные. Принципы и практика построения масштабируемых систем обработки данных в реальном времени / Н. Марц, Д. Уоррен. М.: Вильямс, 2016.

формировать динамику статистических данных идеологических и иных предпочтений.

Коммуникативное информационное онлайн-пространство, онлайн социальная среда, представляющая собой легкодоступное, неконтролируемое, анонимное пространство, становятся благоприятной средой для развития, культивирования, популяризации антиобщественных проявлений. Подобные антиобщественные проявления, переплетаясь между собой, играют значительную роль в процессе мотивации совершения различных правонарушений, преступлений. Так, здесь уместно сказать о:

высоком потенциале возникновения, формирования антиобщественного звена взаимодействия и взаимовлияния;

выстраивании отношений среди лиц несовершеннолетнего и молодого возраста в сфере досуга, носящих девиантный потенциал (распространение, употребление наркотических средств, психотропных веществ, участие в мероприятиях, носящих экстремистский характер);

формировании престижа деятельности, носящей экстремистский характер;

популяризации в молодежной среде и среди лиц несовершеннолетнего возраста криминальной субкультуры;

формировании среди лиц несовершеннолетнего и молодого возраста стереотипов поведения криминогенной направленности.

В целях реализации наиболее эффективных мер предупреждения преступности лиц несовершеннолетнего возраста важно разработать комплекс мер, непосредственно направленных на нейтрализацию воздействия информации, которую данная категория граждан получает в глобальной сети. Одним из направлений предупреждения преступлений экстремистской направленности является вовлечение лиц несовершеннолетнего возраста в общественную деятельность. Осуществление подобной деятельности возможно и на муниципальном, и на региональном уровне.

Представляется, что отдельное внимание следует уделить вовлечению лиц несовершеннолетнего возраста в так называемую хакерскую деятельность. В данном случае становится важным проведение мероприятий, нейтрализующих мотивацию преступного поведения среди несовершеннолетних. Так, в ряду по-

добных мер можно выделить организацию проведения различных интернет-соревнований по программированию с престижными номинациями для победителей, в частности: зачисление (без прохождения конкурсных испытаний) в престижный вуз; прохождение оплачиваемой стажировки в передовых IT-компаниях; трудоустройство после обучения; реализация программ государственного образовательного кредитования либо компенсация затрат на учебный процесс; бесплатное участие в региональных, федеральных, международных профессиональных форумах и т.п.

Надо отметить, что содержание подобных мер криминогенного вовлечения лиц несовершеннолетнего, молодого возраста в хакерство не позволяет ее относить к разряду меры специальной направленности. Эффективность ее реализации подразумевает также исполнение мер общего назначения – организационного, правового, ресурсного обеспечения, если речь идет о государственно-частном партнерстве, которое предусматривает участие разных субъектов (вузы, компании, средства массовой информации, органы государственной власти в сфере образования, безопасности, информационной политики и даже банки) в такой малозаметной, но при этом эффективной мере, носящей профилактический характер.

Сегодня крупные корпорации уже принимают определенное участие в предупреждении преступности лиц несовершеннолетнего возраста[1].

Любопытно, что предупредительное распознавание криминогенных угроз, существующих в жизни лиц несовершеннолетнего возраста, реализуется и иными компаниями, профессиональная деятельность которых напрямую не связана с задачами предупреждения рассматриваемого вида преступности.

Здесь речь идет об исследовании Сбербанка России[2], посвященном установлению основных качественных характеристик, особенностей личности лиц несовершеннолетнего и моло-

---

[1] Среди отечественных компаний динамику постоянства в реализации таких мероприятий проявляют такие телекоммуникационные компании, как «Мегафон», «Билайн», до недавнего времени Yota. URL: http://intalent.pro/article/kak-ustroen-rynok-kibersporta-v-rossii-i-sng.html (дата обращения: 20.02.2021).

[2] Исследование Сбербанка России «30 фактов о современной молодежи». URL: https://adindex.ru/news/researches/2017/03/10/158487.phtml (дата обращения: 21.02.2021).

дого возраста (от 5 до 25 лет). Отдельное внимание было обращено на выявление криминологически значимых явлений, способных детерминировать причинные факторы преступности как внешнего, так и внутреннего значения. Исследование было проведено без участия криминологов, психологов, социологов. Основным источником информации стал анализ упомянутой информационной сферы общения, взаимодействия, взаимовлияния лиц несовершеннолетнего и молодого возраста, а именно: персональных страниц, различных форумов, блогов, коммуникационных сетей общения. Примененный специалистами Сбербанка подход является методом включенного наблюдения, который широко применяется специалистами криминологической науки, социологии, исследующими механизмы взаимодействия, взаимовлияния социальной среды и личности. Так, в результате проведенного исследования полученные результаты ложатся в основу наиболее реалистичного прогноза угроз криминализации лиц несовершеннолетнего возраста, а также принятия мер предупредительного характера в отношении подобных угроз.

Итак, результаты подобных исследований являются информативными в целях выявления перспективных, современных направлений в области предупреждения преступности лиц несовершеннолетнего возраста. Потенциальные возможности таких перспектив, как и потенциал математического моделирования предупреждения преступности в целом[1], находятся в плоскости одного из основных факторов криминогенной направленности, который выражен в информационном содержании однородной по сфере приложения информационной технологии Big Data.

---

[1] См.: *Шишкин С.И.* Использование методов логико-математического моделирования для оптимизации санкций уголовно-правовых норм // Рос. следователь. 2009. № 22; *Пилюгина Т.В., Натура Д.А.* Использование метода математического моделирования при прогнозировании региональной преступности и в вопросах ее предупреждения // Всерос. криминолог. журн. Т. 11. 2017. № 1; *Утаров К.А.* Математические методы в криминологии: автореф. дис. … канд. юрид. наук. М., 2004. С. 20.

Е.В. Михайлова,
старший преподаватель
кафедры криминологии
Московского университета
МВД России имени В.Я. Кикотя,
кандидат юридических наук

Криминологические аспекты преступлений в сфере компьютерной информации, совершаемых несовершеннолетними

Интенсивное развитие информационных технологий, сетей передачи данных, сферы телекоммуникационных услуг, расширение доступности сети «Интернет» способствовало появлению киберпреступности. По объему потенциального ущерба киберпреступность занимает седьмое место в списке основных глобальных рисков, опережая техногенные экологические катастрофы и распространение инфекционных заболеваний[1]. Следует отметить, что киберпреступность характеризуется разнообразием и изменчивостью в связи с непрерывным развитием информационных технологий и совершенствованием возможностей сети «Интернет».

Структурно-динамические изменения статистических характеристик позволяют сделать вывод о ежегодном росте количества преступлений в сфере компьютерной информации в стране: в 2015 г. зарегистрировано 2382 преступления, в 2016 г. – 1748, в 2017 г. – 1883, в 2018 г. – 2500, в 2019 г. – 2883, в 2020 г. – 4498[2]. Однако современное формирование правоприменительной практики по делам о преступлениях в сфере компьютерной информации, их латентность и проблемы статистического учета не дают возможности в полном объеме оценить количественные и качественные показатели киберпреступности.

Киберпространство является базой реализации преступных деяний не только взрослыми, но и несовершеннолетними, поскольку для их совершения обычно достаточно иметь компьютер

[1] Threat Zone'19. URL: https://bi.zone/research/threat_zone_2019/ (дата обращения: 21.01.2021).
[2] URL: https: мвд.рф./reports /item/19412450/ (дата обращения: 02.02.2021).

и выход в сеть «Интернет», где современные подростки проводят большую часть своего времени. Молодые люди готовы на совершение преступных деяний не только из любопытства, желания приобщиться к виртуальному обществу, субкультуре, но и из-за возможности заработка, в том числе путем противоправных действий (взломы аккаунтов в соцсетях с целью шантажа, создание вредоносного программного обеспечения «на заказ»).

Предусмотренные Уголовным кодексом Российской Федерации преступления в сфере компьютерной информации (гл. 28, ст. 272–274) несовершеннолетние способны совершать, не владея определенными знаниями в области программирования, а всего лишь основываясь на собственных навыках, технической осведомленности и доступности информации в данной сфере. Число несовершеннолетних лиц, осужденных за совершение преступлений в сфере компьютерной информации, незначительно, что вызвано высокой латентностью данных преступлений, сложностями обнаружения и фиксации доказательств, а также их многоэпизодностью. Так, в 2016 г. за преступления, предусмотренные ст. 272–274 УК РФ, осуждено 3 несовершеннолетних, в 2017 г. – 6, в 2018 г. – 3, в 2019 г. – 2[1]. В первом полугодии 2020 г. несовершеннолетних, осужденных по указанным статьям, не было.

С точки зрения статистики, преступления, совершенные несовершеннолетними в сфере информационной безопасности, в настоящее время не нашли широкого распространения, однако криминогенная обстановка в данной сфере в условиях дальнейшего интенсивного развития информационных технологий вызывает определенную тревогу и требует принятия соответствующих мер противодействия преступности несовершеннолетних в сфере информационной безопасности.

В целях предупреждения совершения компьютерных преступлений целесообразно заниматься правовым, информационным воспитанием детей путем внедрения в школы программ повышения компьютерной грамотности, стандартов этических нормы поведения в цифровой среде, соблюдения прав других граждан, ограничений, установленных законодательством.

[1] URL: http://www.cdep.ru/ (дата обращения: 20.01.2021).

Чтобы предупредить возможные риски и направить знания и энергию детей в нужном направлении, многие государства готовят специалистов по кибербезопасности со школьной скамьи. Например, в Великобритании проводятся ежегодные молодежные соревнования по кибербезопасности (с целью привлечения детей в 2015 г. одним из этапов соревнований стал специально разработанный уровень популярной компьютерной игры Minecraft)[1]. Австралийское правительство с 2018 г. включило обязательное преподавание блокчейн (blockchain) и криптоалгоритмов в образовательную программу начиная с младших классов, что позволяет дать детям финансовое и цифровое образование[2]. Агентство национальной безопасности США активно использует практику по созданию так называемых отрядов белых хакеров, в которые входят молодые люди, тестирующие программное обеспечение на наличие уязвимости[3].

В 2008 г. в Республике Корея создана Международная федерация киберспорта, который сегодня приобрел огромную популярность во многих странах мира. По компьютерному спорту проводятся соревнования как для профессиональных спортсменов, так и для любителей, в том числе студентов и школьников. Активно развивается киберспорт и в Российской Федерации. С 2006 г. проводятся официальные соревнования для студентов, обучающихся в образовательных учреждениях высшего образования. После официального признания компьютерного спорта в 2016 г. была организована Всероссийская киберспортивная студенческая лига (ВКСЛ)[4].

Для совершенствования навыков специалистов по информационной безопасности организуются международные командные соревнования CTF (Capture the flag) по информационной безопасности и системному администрированию. Крупнейшими между-

---

[1] *Дети* и технологии / Т.А. Аймалетдинов, Л.Р. Баймуратова, В.И. Гриценко, О.А. Долгова, Г.Р. Имаева; Аналит. центр НАФИ. М.: Изд-во НАФИ, 2018. С. 345.

[2] *Долгов С.* Криптотехнологии в детском саду. URL: https://mel.fm/blog/sergey-dolgov/62931-kriptotekhnologii-v-detskom-sadu (дата обращения: 20.01.2021).

[3] Joan Ganz Cooney Center. URL: http://joanganzcooneycenter.org (дата обращения: 20.01.2021).

[4] Официальный сайт Всероссийской киберспортивной студенческой лиги // Федерация компьютерного спорта России, 2000–2021. URL: http://студлига.рф (дата обращения: 20.01.2021).

народными соревнованиями считаются проводимые Калифорнийским университетом в Санта-Барбаре, победителем которых в 2018 г. стала команда студентов Томского государственного университета SiBears.

Правовая пропаганда, правовое просвещение среди учащихся технических образовательных учреждений, будущих программистов, сетевых администраторов и специалистов в области защиты информации, информирование их о действующем уголовном законодательстве и ответственности за указанные противоправные деяния снизят риск появления компьютерных преступников в среде технических специалистов.

Инициаторами образовательных проектов для школьников в России выступают коммерческие и некоммерческие организации, такие как Сбербанк России (Академия искусственного интеллекта[1]), Group-IB (образовательные программы по информационной безопасности[2]), акционерная финансовая корпорация «Система» («Лифт в будущее»[3]), Samsung (IT-школа Samsung[4]). Однако в силу ряда причин (высокая стоимость, отсутствие образовательного центра в регионе проживания, недостаточный уровень базовых знаний) такие проекты недоступны для широкой аудитории школьников.

Следует отметить, что значимая роль в предупреждении компьютерных преступлений несовершеннолетних отводится их родителям. Ведь именно они находятся в постоянном контакте со своими детьми. Проведение профилактической работы среди несовершеннолетних сотрудниками образовательных организаций эффективно в отношении детей старшего школьного возраста, но несовершеннолетние, которые только знакомятся с глобальным информационным пространством, нуждаются в непрерывной индивидуальной работе со стороны своих родителей.

---

[1] Академия искусственного интеллекта для школьников. URL: https://www.ai-academy.ru/ (дата обращения: 20.01.2021).

[2] Киберобразование от IB-Group. // 2003–2021 Group-IB – информационная безопасность и защита от киберугроз. URL: https://www.group-ib.ru/cyber-education.html (дата обращения: 20.01.2021).

[3] *Всероссийская* программа развития человеческого капитала в технологической среде // URL: http://bf.sistema.ru/programs/lift/ (дата обращения: 20.01.2021).

[4] IT-школа Samsung. URL: https://www.samsung.com/ru/ itschool/ (дата обращения: 20.01.2021).

Представляется, что для достижения успеха в вопросе недопущения совершения преступлений в информационной сфере несовершеннолетними особое значение имеют осведомленность родителей в данной области, установка доверительных отношений между родителями и детьми, а также использование специального программного обеспечения, позволяющего не только контролировать, но и ограничивать деятельность ребенка в сети «Интернет» и др. Очевидно, что контроль и подробное разъяснение ответственности за совершение противоправных деяний в информационной сфере, приведение примеров будут способствовать уменьшению количества преступлений, совершаемых несовершеннолетними в данной области. Таким образом, непрерывная и целенаправленная работа с несовершеннолетними является залогом успеха в профилактике совершения компьютерных преступлений подрастающим поколением.

С.И. Винокуров,
ведущий научный сотрудник
НИИ Университета прокуратуры
Российской Федерации,
кандидат юридических наук,
доцент

Предупреждение сексуальной эксплуатации несовершеннолетних в сети «Интернет»

1. Сексуальная эксплуатация несовершеннолетних в сети «Интернет» является транснациональным явлением, поэтому его юридические анализ и оценка должны исходить из базовых положений международного права.

Организация Объединенных Наций (далее – ООН) неоднократно провозглашала, что дети имеют право на особую заботу и помощь. В частности, в Декларации прав ребенка от 20.11.1959 (далее – Декларация) особо подчеркивается, что ребенок ввиду его физической и умственной незрелости нуждается в специаль-

ной охране и заботе, включая надлежащую правовую защиту как до, так и после рождения.

Исключительно важное значение в связи с этим имеет провозглашенный Декларацией принцип, согласно которому «ребенку законом и другими средствами должна быть обеспечена специальная защита и предоставлены возможности и благоприятные условия, которые позволяли бы ему развиваться физически, умственно, нравственно, духовно и в социальном отношении здоровым и нормальным путем и в условиях свободы и достоинства. При издании с этой целью законов главным соображением должно быть наилучшее обеспечение интересов ребенка».

Кроме того, один из принципов Декларации прямо предусматривает, что ребенок должен быть защищен от всех форм эксплуатации и он не должен быть объектом торговли в какой бы то ни было форме.

Еще более определенно, комплексно и детально права ребенка защищены Конвенцией ООН о правах ребенка от 20.11.1989 (далее – Конвенция). Здесь особую значимость приобретает ст. 34 Конвенции, которая предусматривает, что «государства-участники обязуются защищать ребенка от всех форм сексуальной эксплуатации и сексуального совращения. В этих целях государства-участники принимают на национальном, двустороннем и многостороннем уровнях все необходимые меры для предотвращения:

a) склонения или принуждения ребенка к любой незаконной сексуальной деятельности;

b) использования в целях эксплуатации детей в проституции или в другой незаконной сексуальной практике;

c) использования в целях эксплуатации детей в порнографии и порнографических материалах».

Кардинальное значение для защиты детей от сексуальной эксплуатации имеет и Факультативный протокол к Конвенции ООН о правах ребенка, касающийся торговли детьми, детской проституции и детской порнографии от 25.05.2000.

Таким образом, международное право однозначно и категорично стоит на страже защиты наилучших интересов ребенка, в том числе предотвращения сексуальной эксплуатации и сексуального совращения детей.

2. Анализ современной практики развития научно-технического прогресса в сфере информационных технологий выявляет серьезные глобальные риски, угрожающие психическому здоровью и нравственному развитию детей.

В частности, речь идет о виртуальной сексуальной эксплуатации несовершеннолетних в сети «Интернет». Здесь следует отметить, что психическое насилие над детьми и подростками и их виртуальная сексуальная эксплуатация распространились вместе с развитием новых информационно-коммуникационных (компьютерных) технологий.

В 2019 г. Internet Watch Foundation (IWF) – организация, отслеживающая и удаляющая противоправный контент в сети, зафиксировала более 132 тыс. веб-страниц, содержащих сцены сексуального насилия над несовершеннолетними. Из них подавляющее большинство (89%) было «прописано» в Европе, преимущественно в Нидерландах. 3% от общемирового контента такого рода пришлось на Россию.

По данным IWF, с начала года количество сообщений о жестоком обращении с детьми в сети увеличилось почти на 50%. Согласно же данным федерального центра обмена информацией по изображениям США, с января по сентябрь 2020 г. во Всемирной паутине было зарегистрировано 52 млн фотографий и видеоматериалов, связанных с сексуальным насилием над детьми. И это только то, что удалось отследить[1].

Аналогичную ситуацию отмечает и Европол. В 2019 г. он выявил более 1,5 млн подобных изображений и видео. Причем исследования говорят о том, что жертвами сексуальных преступлений все чаще становятся маленькие дети: в 28% случаев это дети младше 10 лет[2].

Особенно резко возросла сексуальная эксплуатация детей в период пандемии. Здесь одним из наиболее серьезных криминогенных факторов, связанных со сферой компьютерных техноло-

---

[1] *Портякова Н.* Одно лечат, другому перечат: в ЕС защита детей уперлась в защиту частной жизни. URL: /https://iz.ru/1102964/nataliia-portiakova/odno-lechat-drugomu-perechat-v-es-zashchita-detei-uperlas-v-zashchitu-chastnoi-zhizni (дата обращения: 20.01.2021).

[2] Новости ООН (03.03.2020). Эксперт по защите детей: интернет значительно облегчил сексуальную эксплуатацию детей. URL: https://news.un.org/ru/story/2020/03/1373571) (дата обращения: 20.01.2021).

гий, стало временное прекращение очных занятий во многих школах и переход на дистанционное обучение. В результате дети начали гораздо больше времени проводить в сети ради развлечения, образования и общения.

В то же время существенное снижение жизненного уровня значительной части населения многих государств в совокупности с отдельными ограничительными мерами по сдерживанию пандемии способствовали росту как спроса, так и предложения в отношении сексуальной эксплуатации детей.

Кроме того, финансовые трудности могут стимулировать у подростков желание и поиски путей заработать деньги с помощью самостоятельно снятых порноизображений или активизации сомнительных контактов в сети «Интернет» с незнакомыми лицами, проявляющими интерес к сексуальным услугам несовершеннолетних. Помимо этого, к изготовлению порноизображений подростков могут принуждать преступники с помощью психологических манипуляций, угроз и других видов давления.

В результате этого получили распространение новые виды сексуальной эксплуатации. Так, за последние несколько лет начался бум платных стримов с сексуальной эксплуатацией детей в реальном времени[1]. В частности, в отчете Интерпола предполагается, что спрос на такие стримы вырастет еще больше, в том числе из-за того, что преступники-педофилы ограничены в международных путешествиях. Интерпол также прогнозирует, что предложение онлайн-стримов с насилием над детьми увеличится, так как дети могут быть по сути заперты дома с теми, кто хочет использовать их сексуальную эксплуатацию для обогащения[2].

Характерно также, что в сети «Интернет» увеличилось число дискуссий об эксплуатации и насилии над детьми. Появились многочисленные сторонники сексуального растления и сексуальной эксплуатации детей. Так, на просторах Рунета без особого труда можно найти сайты эротического содержания об отношениях с малолетними, руководства по растлению детей и подрост-

---

[1] Стрим – потоковое видео, которое транслируется онлайн.

[2] *Во время* пандемии резко возросла сексуальная эксплуатация детей. URL: /https://stop rape.ru/ (дата обращения: 23.01.2021).

ков, а также тематические форумы и группы поддержки для педофилов[1].

Найти и вычислить людей, распространяющих в сети идеологию сексуальной эксплуатации детей, по мнению специалистов, технически реально. Однако в УК РФ не предусмотрена ответственность за пропаганду сексуальной эксплуатации и сексуального совращения детей в сети «Интернет».

В связи с этим следует отметить, что Россия при ратификации Конвенции Совета Европы «О защите детей от сексуальной эксплуатации и сексуальных злоупотреблений» (далее – Конвенция СЕ)[2] сделала ряд оговорок, которые, на наш взгляд, излишне либерализуют некоторые деяния в сфере сексуальных злоупотреблений в отношении детей. В частности, Российская Федерация оставила за собой право не применять нормы Конвенции СЕ относительно уголовной ответственности за предложение, предоставление, приобретение, а также хранение детской порнографии, сознательное посещение порнографических представлений с участием детей и др. Данные оговорки, как представляется, вступают в явное противоречие с ключевым принципом международного права о защите наилучших интересов ребенка.

Следует отметить и противоречивую позицию Евросоюза относительно данной проблемы. Имеется в виду директива ЕС о защите конфиденциальности в секторе электронных средств связи, которая вступила в силу 21.12.2020[3]. Она запретила мониторинг электронной почты, цифровых сервисов в ЕС и существенно ограничила использование программного обеспечения, которое сканирует в том числе и изображения сексуального насилия над детьми. Эта практика стала запрещенной без решения суда.

Представляется, что подобное всеобъемлющее, не содержащее никаких исключений решение ЕС об указанном запрете про-

---

[1] *Чаровская А.* Съезд извращенцев. Кто в интернете пропагандирует секс с детьми? URL: /https://iz.ru/1025721/anastasiia-chepovskaia/sezd-izvrashchentcev-kto-v-internete-propagandiruet-seks-s-detmi (дата обращения: 20.01.2021).

[2] Федеральный закон от 07.05.2013 № 76-ФЗ «О ратификации Конвенции Совета Европы «О защите детей от сексуальной эксплуатации и сексуальных злоупотреблений».

[3] Постановление Европейского парламента и Европейского совета касаемо права на личную жизнь и защиту персональных данных в процессе электронных коммуникаций от 19.10.2017, заменяющее Директиву 2002/58/ЕС о конфиденциальности и электронных средствах связи. URL: https://ru.wikipedia.org/wiki/ (дата обращения: 20.01.2021).

тиворечит Конвенции о правах ребенка, где предусмотрено принятие государствами-участниками всех необходимых мер для предотвращения сексуальной эксплуатации и сексуального совращения детей.

В связи с этим возникает принципиально важная проблема границ и пределов использования современных информационно-коммуникационных технологий (так называемой цифровизации). Цифровизация представляет собой, на наш взгляд, техническое (технологическое) средство (инструмент), предназначенное для эффективной реализации разнообразных и постоянно растущих позитивных потребностей и запросов общества, в том числе в социальных коммуникациях. Значима роль цифровизации и в сфере социального управления экономикой, политикой, культурой и т.д. По своей сущности цифровизация, несмотря на ее исключительную востребованность и важность в деле оптимизации социального управления сложными общественными процессами, является производным, второстепенным ресурсом социума, подчиненным более высоким по уровню значимости ценностям: общественной безопасности и благополучию социума.

Таким образом, границы и пределы цифровизации должны определяться ее пользой в деле реализации главных ценностей жизнедеятельности социума – общественной безопасности и общественного блага. Вместе с тем понятно, что в общественной жизни нередко возникает конфликт между частным и общественным интересами. Для его преодоления обычно следует искать разумный баланс данных интересов.

Однако в наиболее важных принципиальных вопросах, когда возникает серьезный конфликт между реализацией частного интереса, что чревато причинением вреда общественному благу и общественной безопасности, выбор должен быть сделан в пользу общественных ценностей.

Следовательно, если цифровизация причиняет в каких-то аспектах вред (тем более содержит признаки общественной опасности деяний) общественному благу и безопасности, то начальная граница вредоносной практики, на наш взгляд, должна служить пределом указанной цифровизации.

Применительно к нашей теме это означает, что если международное право четко и однозначно предусматривает всемерную

защиту прав и наилучших интересов детей, то, следовательно, если определенные информационно-коммуникационные средства (технологии) наносят ущерб этому приоритетному общественному благу, необходимо использовать эффективные механизмы защиты прав ребенка, способные обезопасить детей от возникающих угроз их благополучию и развитию.

Это означает необходимость не только криминализации наиболее одиозных (общественно опасных) деяний в сети «Интернет» (например, пропаганда сексуальной эксплуатации и сексуального совращения несовершеннолетних), но и использования эффективных контр-информационно-коммуникационных средств, направленных на выявление, предотвращение и пресечение подобных информационных злоупотреблений. Речь, в частности, может идти о специальном мониторинге (сканировании) материалов, размещаемых в сети «Интернет», на предмет выявления и блокирования вредоносного контента, выявления лиц, злоупотребляющих анонимностью и свободой слова в открытых информационно-телекоммуникационных сетях, применении соответствующих мер правового реагирования на выявленные нарушения и злоупотребления и др.

При этом принципиально важно отметить, что, определяя баланс интересов между правом на частную жизнь и правом на безопасную жизнь и благополучие детей, выступающих в качестве реальных потенциальных жертв сексуальных насильников, необходимо, с точки зрения международного права, отдавать приоритет наилучшим интересам ребенка.

Эту позицию разделяют не только многие правозащитные организации, но и крупные технологические компании. В частности, такие интернет-компании, как Google, Microsoft и др., дали понять, что продолжат мониторинг своих платформ в целях выявления контента, связанного с сексуальным насилием над детьми, невзирая на всякие постановления[1].

Вместе с тем возникшее противоречие должно найти разрешение на уровне глобального международного права. С этой целью представляется необходимым, чтобы Комитет ООН по правам ребенка поставил точку в этом юридическом споре.

---

[1] *Портякова Н.* Указ. соч.

Важно также иметь в виду, что Конвенция о правах ребенка была принята более трех десятилетий назад и, естественно, в ней не могли найти отражение те новые информационные вызовы, риски и непосредственные угрозы безопасности и благополучию детей, которые мы наблюдаем сегодня.

За прошедший период в жизни мирового социума произошли гигантские изменения, в том числе в сфере информационно-коммуникационных технологий, и сформировались глобальные вызовы и масштабные риски для безопасности и нравственного развития детей. В связи с этим представляется целесообразной разработка Дополнительного протокола к рассматриваемой Конвенции ООН. В нем должны быть обновлены, конкретизированы реальные меры защиты детей в условиях современной цифровизации социальной жизни и оптимального определения баланса интересов между правом на конфиденциальность частной жизни и правом на безопасную жизнь и благополучие детей.

Л.И. Александрова,
старший научный сотрудник
НИИ Университета прокуратуры
Российской Федерации

Применение информационных технологий для противодействия преступлениям в таможенной сфере

Информационные (цифровые) технологии основательно интегрировались в повседневную жизнь современного общества, в том числе во внешнеэкономическую деятельность (ВЭД), где находят применение новейшие инновационные разработки, робототехника, искусственный интеллект.

Развитие современных технологий выводит на новый уровень и взаимодействие таможенных органов и участников ВЭД. Наиболее существенные преимущества цифровых технологий связаны с оптимизацией процессов таможенного регулирования и таможенного контроля. Электронное декларирование через центры электронного декларирования (ЦЕД), удаленный выпуск и

удаленная оплата таможенных платежей – все эти системы четко организованы и профессионально отлажены. В настоящее время Федеральная таможенная служба (ФТС России) является одним из самых передовых ведомств в России, что во многом связано со спецификой ее деятельности, требующей высокой мобильности принятия решений об обеспечении своевременного выпуска товаров. Именно по этой причине большая часть таможенных операций переводится онлайн. Согласно Стратегии развития таможенной службы до 2030 года[1] (далее – Стратегия развития таможенной службы), направленной на полномасштабную модернизацию таможенной сферы, доля таможенных операций, совершаемых автоматически с использованием информационных технологий, в 2024 г. должна быть увеличена до 50% и в 2030 г. – до 100%.

Вместе с тем нельзя не отметить, что наряду с позитивными достижениями и хорошими перспективами применения в таможенной сфере современных информационных технологий открываются большие возможности и для преступного мира.

Количество преступлений в информационном пространстве неуклонно растет. По информации Генеральной прокуратуры Российской Федерации, только за 6 месяцев 2020 г. их прирост составил 92%, или 225,5 тыс. преступлений, и в ближайшем будущем противоправная активность в этом направлении будет только увеличиваться[2].

Злоумышленники повсеместно разрабатывают все более изощренные схемы подготовки и совершения преступлений. Повсеместное использование цифровых технологий и глобальная информатизация приводят к тому, что классические формы преступности, в частности в таможенной сфере, – мошенничества, контрабанды, уклонения от уплаты таможенных платежей и др. уступают место качественно иной преступности, о чем говорят изменения, происходящие в структуре зарегистрированных преступлений. Только за последние несколько лет в УК РФ был внесен ряд изменений и дополнений. Так, введены ст. 193[1] «Совершение валютных операций по переводу денежных средств в ино-

[1]Утверждена распоряжением Правительства РФ от 23.05.2020 № 1388-р.
[2] URL:https://tass.ru/obschestvo/9032391 (дата обращения: 12.02.2021).

странной валюте или валюте Российской Федерации на счета нерезидентов с использованием подложных документов», ст. 200^1 (Контрабанда наличных денежных средств и (или) денежных инструментов), ст. 200^2 (Контрабанда алкогольной продукции и (или) табачных изделий) и др.).

Кроме того, в условиях развития глобальных мирохозяйственных связей, миграции капиталов и колоссального роста международного пассажиропотока повысились латентность и интеллектуальная проработка противоправной преступной деятельности, характеризующиеся высокой степенью организации и вовлечения представителей различных отраслей экономики.

В настоящее время с помощью интернет-торговли в Россию доставляются огромные товарные партии, что создает большие проблемы в борьбе с преступностью. Введение в экономический оборот на территории России контрафактных товаров путем электронной торговли на практике, по существу, никем не контролируется. Наряду с этим имеют место случаи, когда товары оформляются на подставных физических лиц, выявляются виртуальные «челноки», действующие в обход таможенных правил и пошлин, создаются базы паспортных данных. За виртуальные поставки платятся виртуальные денежные средства без уплаты соответствующих таможенных платежей и налогов. Проведение необходимых оперативно-розыскных мероприятий и процессуальных действий в отношении преступлений, связанных с использованием информационных технологий, является затруднительным в связи с территориальной удаленностью относительно друг друга участников событий, а также удаленностью местонахождения носителей информации, имеющей значение для уголовного дела. Зачастую участники уголовного процесса находятся в разных городах или даже странах.

Противодействие преступлениям в таможенной сфере является одной из важнейших задач таможенных органов России. К правоохранительным функциям таможенных органов относится борьба с контрабандой (пресечение незаконного оборота через таможенную границу Евразийского экономического союза наркотических средств, психотропных веществ, оружия, боеприпасов, культурных ценностей и иных предметов), содействие в борьбе с

международным терроризмом, обеспечение защиты прав интеллектуальной собственности и противодействие коррупции.

Все данные функции направлены на достижение одной из главных задач – обеспечение экономической, и в частности финансовой, безопасности Российской Федерации.

В условиях возникновения ранее неизвестных угроз и вызовов в сфере национальной безопасности, имеющих координированный характер, повышается роль правоохранительной деятельности таможенных органов и возрастает необходимость ее совершенствования. Согласно п. 7 Стратегии развития таможенной службы целью совершенствования деятельности этих органов является наращивание использования функционала информационно-программных средств таможенных органов, системы внутриведомственного и межведомственного информационного взаимодействия для оптимизации производства по уголовным делам и делам об административных правонарушениях. Основными задачами в области совершенствования правоохранительной функции таможенных органов являются формирование запросов и получение сведений с применением информационно-программных средств таможенных органов и иных федеральных органов исполнительной власти для ускорения сроков производства по уголовным делам; автоматизация процессов выявления потенциально возможных рисков принятия неправомерных решений таможенными органами по уголовным делам; при высоком уровне риска блокировка действий по принятию должностными лицами таможенных органов решений сомнительного характера, связанных с расследованием уголовных дел; цифровизация документирования оперативно-розыскной деятельности.

21 ноября 2020 г. утвержден План мероприятий на период 2021–2024 годов по реализации Стратегии развития таможенной службы Российской Федерации до 2030 года, предусматривающий мероприятия по совершенствованию правоохранительной деятельности, и в частности внедрение современных цифровых платформ по своевременному выявлению и установлению всех обстоятельств подготавливаемых и совершенных правонарушений. Также предусмотрено дальнейшее развитие межведомственного электронного взаимодействия с правоохранительными, надзирающими и иными государственными органами Российской Федерации.

В условиях цифровизации деятельности таможенных органов, с введением и становлением системы электронного декларирования правоохранительные органы адаптируются к новым реалиям выявления, предупреждения и раскрытия таможенных преступлений, совершаемых в том числе в киберпространстве. Электронное декларирование товаров осуществляется с помощью ЦЭД, что имеет существенное преимущество, поскольку декларант и инспектор могут находиться на любом расстоянии друг от друга, а товары при этом могут размещаться на любых приграничных терминалах. В случае необходимости таможенного досмотра по поручению инспектора ЦЭД, принявшего декларацию, назначенные досмотры проводятся на тех терминалах, где размещены в данный момент товары. При этом взаимодействие между внутренним и приграничным таможенными постами происходит и в электронном виде, что сокращает и коррупционную составляющую. Внедряются всевозможные онлайн-сервисы для организаций и частных лиц, например удаленный таможенный платеж.

В настоящее время таможенная служба продолжает работать над объединением большого числа отдельно существующих счетов и формированием общего платежного пространства для внешней экономической деятельности.

Важнейшую роль в выявлении и предотвращении преступлений играет аналитическая работа, основанная на современных возможностях поиска, сбора, обработки и глубокого анализа разноплановой информации, позволяющей определять тенденции развития криминогенных процессов, происходящих в таможенной сфере деятельности.

К основным элементам информационной инфраструктуры, существующим в настоящее время в таможенных органах России и используемым для аналитической работы, относятся: Единая автоматизированная информационная система (ЕАИС) ФТС России; Ведомственная интегрированная телекоммуникационная сеть (ВИТС) ФТС России; Система межведомственного электронного взаимодействия (СМЭВ) ФТС России; Электронный архив документов декларанта (ЭАДД); Автоматизированная система внешнего доступа таможенных органов Российской Федерации (далее – АСВД ТО); аппаратно-программные средства

шифрования «Континент», антивирусы Лаборатории Касперского, различные средства анализа уязвимостей, анализа трафика и все, что связано с расследованием инцидентов информационной безопасности.

Следует отметить, что существующие в настоящее время в ФТС России информационные системы, как считают практические работники, по ряду причин не обеспечивают в полной мере потребностей правоохранительных таможенных органов. Так, указывается на отсутствие централизованного сбора информации, аккумулирующего результаты уголовной регистрации в сфере таможенной деятельности, на низкий уровень информационного взаимодействия оперативно-аналитических подразделений (ОАП) с оперативно-розыскными службами иных органов, на отсутствие необходимой ведомственной нормативной базы, регламентирующей деятельность ОАП, системы профессиональной подготовки аналитиков, единой методики оперативно-розыскного анализа[1].

Также имеются проблемы при построении единого пространства доверия между ФТС России и другими надзорными службами, такими как Россельхознадзор по фитосанитарным вопросам, Роспотребнадзор по санитарно-эпидемиологическим вопросам, ФНС России по финансовым вопросам и др.

Не все ведомства находятся на одном уровне развития информационных технологий, что порождает разницу в подходах, в используемом инструментарии и зачастую усложняет синхронизацию информации для обмена. К примеру, ФТС России ориентируется на партии товаров, а Федеральная налоговая служба нацеливается на денежные потоки.

Отдельные таможенные документы нельзя использовать в электронном виде вследствие отсутствия единого пространства доверия и системного оператора, который мог бы этот вопрос курировать. Например, к таким документам относятся документы ЕАЭС, отличающиеся от российских криптографией и электрон-

---

[1] *Яковец Е.Н.* Понятие аналитической работы в сфере оперативно-розыскной деятельности таможенных органов // Тамож. дело. 2020. № 4; *Скородумов П.В., Баданин Д.А.* Построение виртуальной среды экономического моделирования // Вопр. территор. развития. 2015. № 4 (24); *Новости* таможни: постконтроль. TKS.RU – все о таможне. URL: lj.tks.ru/news/nearby/2016/03/11/0003.

ной подписью. Без соответствующих механизмов проверки невозможно удостовериться в их подлинности в электронном виде. Использование электронной цифровой подписи (ЭЦП) остается зоной рисков: нельзя быть уверенным в том, что подписант является именно тем лицом, чью подпись использует, недостаточная грамотность граждан в вопросах информационной безопасности и отсутствие определенных навыков работы с компьютером.

Отсутствует также надлежащий контроль за организациями, предоставляющими ЭЦП. Так, имеют место случаи, когда ЭЦП используется в мошеннических целях путем ее оформления на третье лицо.

ЭЦП в современном обществе является неотъемлемым атрибутом, значительно облегчающим документооборот и для юридических, и для физических лиц. Как считают специалисты, на государственном уровне необходимо усиливать работу в направлении повышения безопасности и защищенности ЭЦП, к примеру, с помощью использования биометрических данных, ужесточения требований при ее предоставлении[1].

В целях продолжения работы по созданию высокотехнологичной таможенной службы в противодействии преступности в сфере ВЭД необходим анализ связанных с применением информационных технологий основных рисков в таможенной деятельности, прежде всего, рисков безопасности, а также рисков фискального характера. Необходимо повышать уровень защищенности информационных ресурсов, расширять спектр мер по обеспечению информационной безопасности, выявлять возможности цифровых технологий в организации взаимодействия таможенных органов с правоохранительными органами в контексте формирования единого канала по борьбе с преступностью.

---

[1] *Зорин А.* Электронная цифровая подпись: риски использования, или как воспрепятствовать ее неправильному использованию. URL:https://www.eg-online.ru/article/432800/ (дата обращения: 10.02.2021).

М.Н. Зацепин,
доктор юридических наук,
профессор

А.М. Зацепин,
вице-президент Российской
криминологической ассоциации,
кандидат юридических наук,
доцент

Совершенствование криминологических механизмов противодействия преступности в условиях цифровой экономики

Социальные реформы нуждаются в информационном обеспечении и осуществлении мер по обеспечению законности, прав и свобод граждан, охране собственности и общественного порядка. Вопросы обеспечения законности, правопорядка, общественной безопасности находятся в совместном ведении Российской Федерации и субъектов Российской Федерации. Основным субъектом безопасности является государство, осуществляющее функции в этой области через органы законодательной, исполнительной и судебной власти.

В последние годы произошло бурное развитие систем телекоммуникаций, всемирной сети «Интернет», которая представляет собой массовую реализацию опосредованной социально-правовой среды, обладающей уникальными характеристиками для криминологических исследований и выработки методологических рекомендаций в механизме противодействия преступности. В качестве основополагающих элементов – новое средство коммуникации, в основе которого лежит способ получения информации потребителями, отличный от традиционных, обладающий высокой гибкостью и масштабностью, а также глобальный электронный рынок, не имеющий каких-либо территориальных или временных ограничений, позволяющий проводить интерактивную социальную и экономическую деятельность. К важнейшим аспектам управления использованием сети

«Интернет» и его правового регулирования относятся вопросы соблюдения и защиты прав интеллектуальной собственности – личных неимущественных и имущественных (исключительных) прав в рамках системы авторского права, смежных и патентных прав. Данные вопросы обсуждаются (признаются) на национальном и международном уровне. Вместе с тем появилась проблема преступности в сфере IT и защиты прав собственности в сети, ставшей основой развития всех сфер общества, составной частью механизма формирования и реализации баланса прав человека в цифровой среде. Последнее, несомненно, представляет собой предмет теоретического и практического интереса[1].

Использование сети «Интернет» в системе социальной и экономической деятельности благодаря его уникальным характеристикам значительно повышает и эффективность деятельности правоохранительных и судебных органов. Ресурсы сети используются в следующих направлениях криминологической деятельности. Это набор возможностей получения информации об объекте исследования, электронные опросы, участие в телеконференциях. Пользователи выделяют три основных способа получения криминологической информации: статистические данные возможно получить при помощи поисковых программ или посредством гипертекстовых ссылок, электронную версию научной публикации, газеты, журнала[2].

Информационная кампания, направленная на оповещение пользователей сети, содержит следующие мероприятия – регистрация, размещение ссылок, публикации, размещение рекламных объявлений, участие в телеконференциях, использование списков рассылки. Информация в сети «Интернет» более дружественна по отношению к пользователям, чем традиционные средства массовой информации. В экспертной среде выделяют и области конфликта и координации, определяющие социаль-

---

[1] *ЦБ рассказал* о борьбе с мошенничеством на финрынке. URL: https://pravo.ru/news/206483/

[2] «…каждое 10 преступление совершается в сфере IT …за первое полгодие 2019 г. из 1 млн преступлений 117 640 совершено с использованием компьютерной информации или интернета…» // Число IT-преступлений выросло в полтора раза. (29.09.2019). URL: https://pravo.ru/news/213655/

ную и экономическую политику через Интернет. Это интеллектуальная собственность, кибербезопасность, регулирование контента и управления интернет-ресурсами. В основе проблем управления и правового регулирования Интернета находится базовый конфликт – коллизия между свободным доступом и контролем над ним. Интернет – пространство, в котором становится очевидной общая проблема цифровой среды, – коллизия между интересами правонарушителей и интересами общества. «Пандемия коронавируса, увы, высветила не только плюсы блогосферы, но и минусы… в этот период участились случаи мошенничества и активизировались те, кто использовал тему распространения инфекции для незаконного извлечения материальной выгоды...». Запретительные меры в соцсетях надо вводить точечно[1].

Связь с общественностью. В Интернете публикуются пресс-релизы и представляется текущая информация о криминогенной ситуации. Эффективно используется в кризисных ситуациях, когда правоохранительные органы нуждаются в срочной реакции и информации о преступном событии. Преимущество проявляется и в возможности информации в реальном времени[2].

Поддержка социальных запросов существенно расширена за счет размещения дополнительной публичной информации (статистической и другой) и реализации механизма дополнительной обратной связи, проведения криминологических исследований. Основные методы и инструменты проведения криминологических исследований: использование тематических серверов, проведение опросов, анкетирование посетителей собственного сайта (сервера), исследование конференций, использование данных опросов, проводимых на других серверах (сайтах). Наряду с перечисленными элементами одной из главных особенностей системы исследований в Интернете является получение интерактивной криминологически значимой информации. «Коронавирус воздействует на общество и экономическую

[1] Парламентская газета «РФ СЕГОДНЯ». URL: https://www.pnp.ru/social/

[2] *Более 200* нарушений прав журналистов зарегистрировали в РФ в 2019 году. URL: https://pravo.ru/news/221368/

ситуацию. Но не меньший эффект эпидемия оказывает на организованную преступность и нелегальный рынок. Чем ответит преступный мир на вирус, как изменится функционирование преступных сетей и какой будет институциональная реакция на новые вызовы…»[1].

Всевозрастающее внедрение компьютеров в нашу жизнь расширило диапазон преступной деятельности в сфере высоких технологий. Сегодня необязательно грабить банк, достаточно взломать код доступа к его компьютерной сети. Преступная группа, занимающаяся кражами и грабежами, может натворить меньше бед, нежели компьютерная мышь. По способу совершения преступлений в сфере высоких технологий выделяют наиболее «популярные» средства и методы: запуск компьютерных вирусов, размещение на сайтах рекламы хакеров, подавление информационного обмена в телекоммуникационных сетях, взлом компьютерных кодов, в том числе кодов доступа, банковских реквизитов, похищение информации о персональных данных граждан, так называемый троянский конь – различного рода ошибки, сознательно вводимые преступниками в программное обеспечение компьютерных систем.

В современном информационном обществе почти все преступления могут совершаться и совершаются с помощью высоких информационных технологий. Стремительное развитие компьютерной технологии и международных компьютерных сетей как неотъемлемой части современной международной финансовой и банковской деятельности создало предпосылки, в немалой степени облегчающие совершение экономических преступлений как внутри страны, так и на международном уровне. Незаконное снятие денег с банковских счетов и переброс их на другие счета, отмывание грязных денег, осуществление преступных связей, распространение компромата на конкурентов и тому подобные махинации представляют серьезную угрозу главным образом потому, что обнаружение такого рода преступлений очень затруднено, потому как следы проникновения, взлома немедленно уничтожаются или стираются. «…расследование

[1] *Как пандемия* влияет на преступность. URL:https://pravo.ru/news/220475/

этой категории дел отличается «особой сложностью, связанной с организационными трудностями. Это обусловливается не только спецификой и неочевидностью киберпреступлений, но и присущим им межрегиональным и международным характером»[1].

Как подчеркивается в публикациях уголовно-правового и криминалистического характера, наиболее значимыми для криминологических исследований киберпреступлений являются признаки способов совершения преступления. Универсальных способов подготовки или сокрытия преступлений не существует. Прежде всего это объясняется разнообразием способов, которыми характеризуются виды преступной деятельности, возможностью совершения различных преступлений одинаковыми способами, средствами и т.п. Поэтому не встречается каких-либо развернутых криминологических исследований преступлений по способу их совершения, в том числе и совершаемых в банковской, финансово-кредитной и т.п. сфере и тем более сопряженных с банковскими технологиями. «Среди новых угроз – мошенничества с использованием сотовой связи, а также средств IT-телефонии. Преступники научились подменять подлинные телефонные номера кредитных организаций, государственных служб, выдавая себя за их работников. В прошлом году число противоправных деяний, совершенных с применением информационных технологий, увеличилось в два раза, в январе – сентябре текущего года – почти на 70%»[2].

Уголовное законодательство включает в себя нормы, направленные на защиту компьютерной информации (ст. 272 УК РФ). Преступное деяние, выразившееся в неправомерном доступе к компьютерной информации, посягает на общественную безопасность и общественный порядок, которые являются видовым объектом всех преступлений в сфере компьютерной информации, предусмотренных гл. 28 УК РФ.

---

[1] *В СК* создали отдел по расследованию киберпреступлений. URL: https://pravo.ru/news/217134/

[2] *МВД* создаст подразделения по борьбе с преступностью в сфере IT. URL:https://pravo.ru/news/215771/

Мошеннические действия разнообразны и могут совершаться в различных отраслях и сферах деятельности. Насколько многообразна экономическая жизнь общества (торговля, сфера услуг, недвижимость, банковские операции, рынок ценных бумаг и т.д.), настолько разнообразны возможности для совершения мошеннических действий. Объектом мошенничества являются общественные отношения всех форм собственности (частной, государственной, муниципальной и т.д.). Экономическая категория собственности регулируется нормами ГК РФ. Содержанием права собственности являются права владения, пользования и распоряжения своим имуществом. Предметом мошенничества выступает имущество, которое в наиболее общем виде определяют как материальный, овеществленный труд человека, имеющй материальную ценность и обладающий экономическим свойством стоимости. ГК РФ относит к вещам и деньги, они являются предметом мошенничества как особый эквивалент стоимости, выражающий цену любых других видов имущества, которое может быть движимым и недвижимым. Объективная сторона выражается либо в хищении чужого имущества, либо в приобретении права на имущество. В законодательное определение хищения включены признаки: чужое имущество, его изъятие и (или) обращение в пользу виновного или других лиц, противоправность, безвозмездность, причинение ущерба собственнику или иному владельцу, корыстная цель. Субъективная сторона характеризуется прямым умыслом и корыстной целью. Субъектом мошенничества может быть вменяемое лицо, достигшее 16-летнего возраста.

В группу экономических преступлений входят деяния, именуемые информационными (цифровыми) преступлениями, которые определяют как корыстные посягательства на финансовые ресурсы банков и физических лиц. Потребности практической деятельности органов расследования предопределяют необходимость построения единой криминалистической классификации преступлений, совершаемых с использованием сети «Интернет» в банковских технологиях. При этом необходимо решить криминологическую задачу: выявить специфические признаки, характеризующие определенную разновидность ин-

формационных преступлений, и разработать с их учетом методические рекомендации, которые могут быть в последующем использованы при расследовании преступлений, входящих в ту или иную группу. «Интернет-мошенники рассчитывают остаться безнаказанными. Так оно и выходит»[1].

Анализ научных и других информационных источников показал, что вопросы преступлений, совершаемых с использованием цифровых технологий, не подлежали активному криминологическому исследованию. Правоохранительные органы при квалификации сталкиваются с неразрешимыми проблемами, которые в общем виде можно охарактеризовать как отсутствие системного подхода при классифицировании преступлений.

Понятие преступлений, совершаемых с использованием интернет-технологий, может охватывать несколько криминалистически сходных видов преступлений по способу совершения преступления как одного из элементов состава преступления. Выделяемая на базе классификация экономических преступлений (совершаемых в сфере экономики) является их подсистемой, эта группа деяний выступает в качестве одного из объектов, изучаемых в криминалистике. Основная задача криминологических исследований в криминалистических методиках – определение общих признаков данного объекта и разработка с учетом полученных новых знаний методических рекомендаций по расследованию каждого вида преступлений, совершаемых с использованием высоких цифровых технологий, рассчитанных на их использование правоохранительными органами[2].

Другой особенностью компьютерных преступлений, еще более затрудняющей установление факта незаконного проникновения, является использование международных спутниковых сетей телекоммуникаций и связи, что позволяет совершать такие преступления «быстро за минуты», находясь на значительном расстоянии от самого объекта. Расследование же подобных преступлений, напротив, занимает недели, если не месяцы, давая возможность преступнику предупреждать принимаемые

---

[1] *Аферистка* Ксюша // Рос. газ. 2016. 10 марта.

[2] *Калятин В.О.* О некоторых тенденциях развития законодательства об ответственности интернет-провайдеров // Закон. 2012. № 7.

против него меры. «…зарегистрировано 29 248 преступлений, на 3,8% больше, чем годом ранее. Из них чуть менее половины небольшой тяжести, а 23,5% – тяжкие или особо тяжкие. Почти все зарегистрированные преступления – городские (89,9%), в селах официально совершено 2959 преступлений. За полгода из-за криминала погибли 283 человека, 400 получили тяжкие травмы. На долю интернета приходится 22,7% от общего числа преступлений, и это на 85,4% больше, чем в прошлом году. Это в основном хищения с карт, торговля наркотиками, мошенничества, кражи».[1]

Задача защиты компьютерных систем от несанкционированного доступа и уничтожения программ и баз данных становится особенно актуальной на пороге нового века «искусственного интеллекта», обещающего массовый переход на методы электронного управления технологическими процессами в производстве, что приведет (это уже очевидно сегодня) к появлению принципиально нового вида преступности. «Малый бизнес часто становится легкой добычей киберпреступников. Как этого избежать?»[2]

На многочисленных хакерских серверах и сайтах открыто размещаются программы для взлома и компьютерных атак, что, несомненно, провоцирует асоциальных лиц копировать такие программы и применять их. Наметилась тенденция к использованию услуг хакеров организованными преступными группами, которые создают специализированные офисы, разрабатывают современные электронные технологии для подготовки и совершения преступлений, закладывая и пути ухода от ответственности[3].

Среди преступлений в области высоких технологий незаконные производство, сбыт и приобретение специальных технических средств, предназначенных для негласного получения информации. К ним, в частности, относятся приборы, использу-

---

[1] *Криминальные* итоги полугодия: интернет-преступность набирает обороты, число квартирных краж упало. URL:https://newdaynews.ru/ekaterinburg/696723/

[2] Деловой квартал № 04 (996) // Уволенный сотрудник может заблокировать работу вашей компании.

[3] Информационное агентство «Накануне.RU» // В Москве количество IT-преступлений выросло на 30%. URL:https://pravo.ru/news/221159/

емые для снятия и расшифровки информации, так называемые жучки, скрытые мини-камеры, микрофоны. Продажа таких приборов является преступлением, но оборот технических и радиотехнических спецсредств не прекратился, а перешел в сферу промышленную и далекую от законности.

Причин несколько. Субъективный фактор низкой оснащенности российских правоохранительных органов специальными аппаратными и программными средствами, которые должны если не превышать, то хотя бы соответствовать уровню оснащенности преступников. Другой фактор временной – недостаток опыта и оперативного мастерства сотрудников правоохранительных органов и особая сложность установления самого факта совершения преступления. В настоящее время уровень латентности компьютерных преступлений очень высок, есть основания считать, что он свыше 70% от общего количества совершенных преступлений. В значительной степени это связано с незнанием большинством пользователей компьютеров, предпринимателей, финансистов того, где возможно найти защиту от электронных мошенников, хотя правовая база сегодня позволяет бороться с преступлениями в сфере высоких технологий достаточно эффективно. Тем не менее законодателю необходимо совершенствовать российскую нормативно-правовую базу для соответствия объективно складывающейся реальности и устанавливать санкции, адекватные общественной опасности современной киберпреступности[1].

Основная причина высокой латентности данного вида преступлений в том, что люди иногда не подозревают, что стали жертвами кибернетического преступления (особенно когда речь идет о похищении информации или введении в программу ошибки). Чаще всего предполагают, что произошел обыкновенный сбой программы, и не предпринимают необходимых мер безопасности. Поняв, что их сеть или они подверглись атаке, потерпевшие далеко не всегда обращаются в правоохранительные органы. Например, компании из соображений информационной огласки. Правоохранительные органы гарантируют кон-

[1] *Пленум ВС*: как накажут за использование поддельных дипломов и справок. URL:https://pravo.ru/story/228370/

фиденциальность, но многие компании и банки не желают вмешивать в свои проблемы кого-то со стороны. Если станет известно, что какой-то банк имеет слабую систему защиты от преступников в сфере высоких технологий, то большинство клиентов предпочтут обслуживаться у конкурентов[1].

Бороться с преступностью в сфере высоких технологий лучше всего профилактическими методами. Не искать и сажать преступников по быстро остывающим следам, а создавать такую систему защиты, которая препятствовала бы злоумышленникам, выявляла и устраняла бы возможные пробелы и т.д. Интернет-мошенники как правовое явление и объект административного, уголовного изучения для общественной безопасности стали предметом серьезных научных исследований сравнительно недавно. Традиционная для нашей страны система мер борьбы с правонарушениями, опиравшаяся на развитую структуру социального контроля над любыми формами противоправного поведения, ушла в прошлое, а проблемы обеспечения общественной безопасности в стране вышли за рамки узковедомственных.

«Регулятор потребовал от кредитных организаций предоставить статистику о мошеннических действиях с использованием ЭЦП. В частности, банки раскроют величину ущерба от таких преступных схем»[2].

Что касается существующих институтов противодействия преступности в сфере IT и появившейся в связи с этим угрозе криминализации в сфере общественных отношений, складывающихся в процессе реформирования социально-политического устройства и экономической деятельности, то без научных криминологических исследований невозможно достигнуть того положения, которое обеспечило бы коренной перелом в деле укрепления правопорядка и обеспечения как личной безопасности человека, так и общественной безопасности на территории Российской Федерации. Необходимо осуществление дополни-

---

[1] *Кибермошенники* лишили свердловчан 80 млн рублей. URL: https://newdaynews.ru/ekaterinburg/709642/

[2] *Банки* отчитаются о мошенничествах с цифровыми подписями. URL: https://pravo.ru/news/214242/

тельных государственных мер, направленных на предотвращение либо снижение вероятности возникающих угроз, вызовов и рисков в сфере общественной безопасности от киберпреступлений. «Объем российского рынка высокотехнологических преступлений в финансовой отрасли сократился за последний год на 85%, до 510 млн руб. Об этом говорится в отчете Hi-Tech Crime Trends, подготовленном в пятницу компанией в сфере расследования и предупреждения киберпреступлений Group-IB»[1].

Е.М. Тимошина,
старший научный сотрудник
НИЦ № 1 ВНИИ МВД России,
кандидат юридических наук

Противодействие самоубийствам несовершеннолетних, вызванным влиянием интернет-контента

Исследуемая проблема актуализирована результатами опроса сотрудников полиции, работающих в сфере профилактики правонарушений несовершеннолетних (далее – эксперты), которые отметили тенденцию роста количества суицидов несовершеннолетних в возрасте от 11 до 17 лет из социально благополучной среды, опосредованных влиянием интернет-контента.

Термин «опосредованное влияние» используется в связи с тем, что способом склонения несовершеннолетних к совершению самоубийства выступают не уговоры, предложения, подкуп, обман или иные действия, предусмотренные ст. 110[1] УК РФ (склонение к совершению самоубийства или содействие совершению самоубийства), а умышленное и сознательное воздействие через музыку, рассказы, истории, компьютерные и ролевые игры, диалоги, намеренно формирующие депрессивно-суицидальный контент в интернет-сообществах и чатах, которыми пользуются дети. Полагаем, что такая криминальная деятельность осуществляется с учетом особенностей детской психики, воздействие на которую сказывается негативным образом.

[1] *Число* киберпреступлений в России снижается. URL: https://pravo.ru/news/216516/

Отличительной особенностью несовершеннолетних, о которых нам стало известно, попавших под влияние такого контента и совершивших самоубийство, является их принадлежность к социально благополучной среде: все они имели теплые семейные взаимоотношения и налаженные контакты в иных референтно-значимых группах, были в полной мере социализированы, положительно характеризовались по месту учебы (многие учились на хорошо и отлично), имели разнообразные интересы (занимались в кружках и секциях музыкой, спортом, рисованием, танцами и пр.), они и их родители не состояли на профилактическом учете в подразделениях по делам несовершеннолетних органов внутренних дел (далее – ПДН). Эти дети решились на самоубийство без видимых на то причин, а у окружающих их людей не было оснований даже заподозрить такую возможность. Они, как правило, оставляли трогательные записки родителям («Мамочка и папочка, я вас очень люблю. Простите меня. Но мне незачем дальше жить»[1]) и эмоционально тепло прощались с друзьями («Я хотела сказать, что всех вас люблю… ну а вообще я хочу жить… и всегда хотела, но осознала это слишком поздно»[2]).

Учитывая приведенные факты, имеются основания предположить, что у этих детей действительно отсутствовали проблемы коммуникативной сферы или социализации, а также реальные причины для смерти. Тем не менее они преждевременно ушли из жизни под влиянием депрессивно-суицидального контента, намеренно распространяемого в интернет-сообществах и аккаунтах. По мнению экспертов, смертность от суицидов без видимых причин у несовершеннолетних чаще, чем у лиц в возрасте старше 18 лет.

Сказанное свидетельствует о том, что под влиянием новых криминальных угроз появились отдельная категория жертв преступлений – *несовершеннолетние из социально благополучной среды, совершающие (совершившие и пытающиеся совершить) самоубийства под влиянием депрессивно-суицидального интернета-контента,* и малоизученная виктимологическая проблема.

---

[1] Из предсмертной записки школьницы Н. 12 лет (январь 2021 г.).

[2] Написала девочка А. 11 лет в социальной сети после принятия смертельной дозы таблеток (январь 2021 г.).

Традиционно причины самоубийств несовершеннолетних связывали с проблемами их социального неблагополучия, сложностями коммуникации, психическими отклонениями, вокруг которых и выстраивали систему профилактической работы. Однако реальность приводит к выводу о необходимости пересмотра системы предупреждения данного опасного явления с учетом появления нового причинного комплекса.

Подразделения по делам несовершеннолетних органов внутренних дел выявляют лиц, склоняющих несовершеннолетних к суицидальному поведению[1]. Однако данная работа строится вокруг реальной, а не виртуальной социальной действительности. Например, на основании информации, полученной из образовательной организации, строится профилактическая работа с несовершеннолетним, проявляющим суицидальное поведение. Несмотря на то что такую работу нельзя назвать ранней профилактикой, даже она не включает мониторинг активности ребенка в социальных сетях и детальное изучение воздействующего на него интернет-контента. Проверки по фактам самоубийства детей также связаны с обстоятельствами реальной действительности, которые могли быть или должны были быть известны сотруднику полиции и по которым тот не принял своевременных и эффективных мер.

Не способствует выполнению задач предупреждения самоубийств несовершеннолетних и отсутствие методики проведения профилактических мероприятий для сотрудников правоохранительных органов (в первую очередь ПДН) после получения ими информации о суицидальном поведении ребенка.

Существенной проблемой в профилактике суицидального поведения несовершеннолетних эксперты назвали отсутствие разработанных и утвержденных *методик выявления суицидального поведения в сети «Интернет»*. По их мнению, данные инструкции необходимы, поскольку подростки больше раскрываются при общении в виртуальной среде. В реальном мире несовершеннолетний может не проявлять суицидальных желаний и поведения, что не позволяет своевременно его выявить, отреаги-

[1] Пункт 2 ст. 21 Федерального закона от 24.06.1999 № 120-ФЗ «Об основах системы профилактики безнадзорности и правонарушений несовершеннолетних».

ровать на сложившуюся ситуацию и предпринять профилактические меры воздействия. В сети «Интернет» ребенок ведет себя совсем иначе и свободно высказывает свои мысли, в том числе по поводу желания уйти из жизни, депрессивных состояний, с легкостью раскрывается «виртуальному другу», которого никогда не встречал в реальной социальной действительности.

Следует отметить, что в России отсутствует механизм мониторинга сети «Интернет» для выявления сообществ и аккаунтов, создающих депрессивно-суицидальное пространство в целях склонения несовершеннолетних к совершению самоубийства. В то же время в ряде стран существует положительный опыт распознавания опасного для детей контента разного вида[1].

Борьба с данным негативным явлением, по нашему мнению, должна затронуть и вопрос совершенствования практики выявления и расследования преступлений. Сегодня сложно возбудить уголовное дело по ст. 110^1 УК РФ. Это означает, что виновные лица уходят от ответственности, что делает борьбу с их преступной деятельностью практически неосуществимой. Указанная ситуация обусловлена сложностью установления причинно-следственной связи между самоубийством несовершеннолетнего и влиянием на него депрессивно-суицидального контента в сети.

Возможно, это связано с пробелом правовой регламентации и отсутствием дополнительного признака состава преступления, предусмотренного ст. 110^1 УК РФ, – такого самостоятельного способа его совершения, как «воздействие на несовершеннолетнего с помощью депрессивно-суицидального контента», который должен рассматриваться как реальная угроза, способствующая совершению самоубийств детьми.

Не исключено, что эту ситуацию усугубляет «палочная система», при которой для формирования высоких показателей выгоднее не обнаруживать в социальных сетях признаки указанного преступления (с учетом трудности его раскрытия), а оформить отказной материал по результатам проверки. Очевидность изменения подходов к формированию показателей работы сотрудни-

---

[1] *Жданов Ю.Н., Овчинский В.С.* Киберполиция XXI века: международный опыт. М.: Междунар. отношения, 2020. С. 103.

ков правоохранительных органов в этой сфере не вызывает сомнений.

Так, в результате опроса родителей, ребенок которых (по всем признакам из социально благополучной среды) совершил самоубийство, было установлено, что, обнаружив после смерти дочери в ее социальных сетях прямые инструкции совершения самоубийства, родители написали заявление о проведении дополнительной проверки по факту ее смерти, по результатам которой тем не менее было принято решение об отказе в возбуждении уголовного дела.

Полагаем, что в ходе проверки по факту самоубийства несовершеннолетнего в обязательном порядке внимание должно уделяться изучению содержимого социальных сетей на предмет обнаружения признаков склонения к совершению суицида или содействия его совершению, в том числе с помощью воздействия депрессивно-суицидального контента.

Считаем целесообразным в деятельности по противодействию самоубийствам несовершеннолетних использование ресурса общественных организаций, совместными усилиями которых регулярно предотвращаются готовящиеся самоубийства детей[1].

Рассмотренная проблема серьезна не только в связи с тем, что представляет угрозу для жизни детей, но и по причине отсутствия у общества и правоохранительных органов необходимого потенциала для ее решения. Очевидно, что высокие технологии, используемые в криминальных целях, обусловливают необходимость пересмотра не только способов, но и всей стратегии борьбы с преступностью, основным направлением которой должно стать активное использование современных компьютерных технологий и международного сотрудничества.

[1] АНО «Родители за чистый интернет». URL: https://vk.com/zachistiyinternet (дата обращения: 01.02.2021).

Т.Ю. Изгагина,
старший научный сотрудник
НИИ Университета прокуратуры
Российской Федерации

Использование цифровой валюты в преступной деятельности и меры по противодействию криминальному рынку биткоина

Отсутствие правового регулирования в отношении цифровой валюты, контроля за ее оборотом, анонимность в вопросах совершения финансовых операций с использованием данного средства платежа повлекли возникновение нового вида преступности – незаконного оборота и контрабанды биткоинов.

В 2019 г. Россия стала мировым лидером по объему торгов на платформе LocalBitcoins. За период с 1 января 2017 г. по 1 октября 2019 г. пользователи LocalBitcoins осуществили сделок на 1,6 млн BTC. На Россию пришлось почти 25% всего объема. За ней следуют США (17,8%) и Китай (13,1%). В неделю российскими пользователями на LocalBitcoins совершалось в среднем сделок на 800 BTC в мае 2020 г., для сравнения еженедельная средняя сумма сделки пользователей Венесуэлы и США – 400 BTC. Количество активных адресов биткоина в ноябре 2020 г. достигло показателя 1,18 млн, что соответствует максимуму, достигнутому в конце 2017 г. (1,29 млн), при этом количество отправляющих адресов достигло рекордного уровня 836 084. Приведенные данные свидетельствуют об активизации деятельности по купле-продаже биткоинов.

Биткоин используется при совершении ряда преступлений как средство платежа за поставленные незаконные товары и оказанные услуги, поскольку важным преимуществом операций с биткоином является их анонимность. В ряде исследований отмечается, что виртуальные валюты (криптовалюты) могут использоваться для финансирования терроризма[1], экстремистских вы-

[1] *Бывший* аналитик ЦРУ: исламские террористы начали использовать биткоин для сбора средств. URL: https://forklog.com/byvshij-analitik-tsru-islamskie-terroristy-nachali-ispolzovat-bitkoin-dlya-sbora-sredstv/ (дата обращения: 11.11.2020).

ступлений, иностранных агентов, ведущих деятельность на территории Российской Федерации. Например, деятельность Фонда борьбы с коррупцией А. Навального финансировалась в биткоинах путем перевода их на электронный кошелек[1]. Рынки Даркнета продают наркотики за криптовалюту[2] (одним из популярных ресурсов является так называемая Гидра). Использование цифровых технологий, по мнению правоприменителей, не увеличивает число преступлений, а облегчает способы их совершения, делая их бесконтактными. К сожалению, борьба с криптомаркетами в Даркнете в России практически не ведется, о чем свидетельствует отсутствие уголовных дел в отношении их основателей.

Криптовалюта используется в совершении коррупционных преступлений, преступники используют электронные платежные системы, такие как «Яндекс. Деньги», «Киви-кошелек»[3]. В связи с этим в 2019 г. в постановление Пленума Верховного Суда Российской Федерации от 09.07.2013 № 24 «О судебной практике по делам о взяточничестве и об иных коррупционных преступлениях» были внесены изменения[4], в соответствии с которыми моментом окончания получения или дачи взятки является в том числе момент зачисления передаваемых ценностей на электронный кошелек.

Криптовалюты являются инструментом отмывания незаконных средств. В связи с необходимостью формирования единообразной практики привлечения к ответственности за легализацию с использованием криптовалют было принято постановление Пленума Верховного Суда Российской Федерации от 26.02.2019 № 1 «О внесении изменений в постановление Пленума Верховного Суда Российской Федерации от 7 июля 2015 года № 32 «О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого

---

[1] *Средства* были похищены. Почему СК обвинил Навального в мошенничестве? URL: https://aif.ru/politics/world/sredstva_byli_pohishcheny_pochemu_sk_obvinil_navalnogo_v_moshennichestve (дата обращения: 28.01.2021).

[2] *Криптовалюты,* наличные деньги и наркотики: исследование. URL: https://1bitcoin.wiki/articles/crypto-cash-and-drugs-crypto-use-grows-as-drug-trade-digitalizes/; *Долгиева М.М.* Криптовалютная наркоторговля в России и за рубежом // Вестн. Воронеж. ин-та МВД России. 2018. № 4.

[3] *Верховный* суд уточнил, что токены могут быть предметом взятки. URL: https://tass.ru/obschestvo/7411147 (дата обращения: 30.11.2020).

[4] Постановление Пленума Верховного Суда РФ от 24.12.2019 № 59.

преступным путем», которое отнесло к предмету преступлений, предусмотренных ст. 174 и 174[1] УК РФ, «денежные средства, преобразованные из виртуальных активов (криптовалюты), приобретенных в результате совершения преступления».

Цифровая валюта активно используется для вывода капитала за рубеж. За биткоины за рубежом давно приобретаются предметы роскоши, недвижимость (впервые такая сделка прошла в Канаде в 2013 г.), в биткоинах выплачивается заработная плата, созданы даже платформы по поиску работы, которая оплачивается в цифровых валютах (например, Bitgigs.com, Coinality, Cryptojobslist, Crypto.jobs, Cryptocurrencyjobs.co)[1]. В связи с изложенным отрицать факт, что цифровая валюта заняла место на мировой арене как средство платежа, бессмысленно.

В России при отсутствии правовой регламентации оборота цифровых валют начала складываться правоприменительная практика по противодействию незаконному обороту биткоина. Например, в 2017 г. по ч. 2 ст. 172 УК РФ возбуждено уголовное дело в отношении группы лиц, организовавших площадку для обмена криптовалюты. Преступники оформили около 300 карт-счетов и SIM-карт на знакомых лиц и осуществляли переводы и обмен криптовалюты. За обналичивание средств они удерживали от 0,5% от суммы. За период с 2015 по 2017 г. ими было обналичено 530 млн руб., доход составил 2,5 млн руб. Суд вынес обвинительный приговор троим соучастникам по ст. 171 УК РФ (Незаконная предпринимательская деятельность). Согласно приговору в доход государства со ссылкой на п. «е» ст. 2 Конвенции ООН против транснациональной организованной преступности были обращены денежные средства, находящиеся на учетных записях в платежной системе Visa QIWI Wallet, на которые был наложен арест[2].

Цифровые активы зачастую выступают в качестве предмета преступления. По данному вопросу правоприменительная практика не единообразна.

---

[1] URL: https://www.rbc.ru/crypto/news/5d4be8b79a794782f579d736 (дата обращения: 12.11.2020).

[2] Приговор Свердловского районного суда Костромской области от 16.07.2018 по делу № 1-416/2017. URL: https://sudact.ru/regular/doc/BpRtLg3cn3ZW/ (дата обращения: 11.11.2020).

Например, в Марий Эл возбуждено уголовное дело по факту присвоения средств с использованием сайта-двойника официального сайта биржи криптовалют, через который потерпевший пытался приобрести биткоины, для чего перевел на счет мошенников 100 тыс. руб. После этого сайт оказался заблокированным, а на счет продавца биткоины не поступили. Преступные действия были квалифицированы как мошенничество[1].

В то же время Петроградский районный суд г. Санкт-Петербурга при рассмотрении уголовного дела, возбужденного по факту хищения имущества, среди которого были в том числе биткоины, которые жертва перевела похитителям, исключил данные активы из суммы причиненного ущерба, поскольку «криптовалюта не является предметом преступления против собственности, в связи с отсутствием правового статуса признать ее объектом гражданского права не представляется возможным, данный вид виртуальных денежных средств не подпадает ни под одну из категорий, не является признанным средством платежа на территории РФ, законодателем отнесена к суррогатам денежных средств»[2].

По исковому требованию обязать обеспечить возврат криптовалюты на цифровые кошельки Арбитражный суд города Москвы отказал в удовлетворении иска в полном объеме, указав, что проведение российскими гражданами и организациями операций с использованием криптовалюты не защищено законами России. Поскольку правовой статус криптовалют не определен, существо отношений, связанных с оборотом криптовалют, не позволяет применить к криптовалютам по аналогии нормы, регулирующие сходные отношения[3].

Таким образом, в приведенных решениях установлено, что права владельцев цифровых валют на территории Российской Фе-

---

[1] *Возбуждение* уголовных дел по криптовалюте и майнингу. URL: https://bitcryptonews.ru/lawyers/vozbuzhdenie-ugolovnyix-del-po-kriptovalyute-i-majningu (дата обращения: 12.11.2020).

[2] URL: https://yandex.ru/turbo/beincrypto.ru/s/rossijskij-sud-ne-schitaet-krazhu-bitkoinov-prestupleniem/ (дата обращения: 12.11.2020).

[3] Постановление Девятого арбитражного апелляционного суда от 04.02.2020 № 09АП-76537/2019 по делу № А40-164942/19. URL: https://kad.arbitr.ru/Document/Pdf/db741b81-cf91-4880-99b3-140e4b4e15c1/51908f57-efef-445c-9e67-16fb71badc1a/A40-164942-2019_20200204_Postanovlenie_apelljacionnoj_instancii.pdf?isAddStamp=True (дата обращения: 12.11.2020).

дерации не защищаются. Для сравнения: в США гражданин Украины был приговорен к девяти годам тюрьмы за кражу более чем 10 млн долл. в цифровой форме у своего бывшего работодателя[1].

В Федеральном законе от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» даны понятия цифровых финансовых активов и цифровой валюты. Приняв закон, государство предпринимает попытку упорядочить деятельность, связанную с оборотом биткоина в России, поскольку в настоящее время вся данная деятельность и доходы от нее целиком и полностью находятся в теневом секторе экономики. Эксперты отмечают, что многие термины, используемые криптосообществом, не закреплены в законе № 259-ФЗ, вместо них вводятся новые правовые институты, которые создают неопределенность; ряд сфер остался неурегулированным, прежде всего, майнинг – процесс создания новых криптоденег. Право на судебную защиту своих прав на цифровую валюту поставлено в зависимость от исполнения обязанностей по уплате налогов (информировании о наличии цифровой валюты и сделок с ней). А определение цифровой валюты противоречит положениям ст. 14 данного закона, где фактически установлен запрет на определенные сделки с криптовалютой (продавать за криптовалюту). В то же время никакой ответственности за нарушение данного запрета не установлено. В связи с этим необходимо предусмотреть ответственность за нарушение порядка обращения цифровых активов и цифровой валюты, как это сделано для валюты Российской Федерации и иностранной валюты. В условиях, когда рынок биткоина уже криминализировался, необходимо предусмотреть возможность осуществления контроля над указанными операциями, используя имеющиеся наработки, рекомендации, а также возможности сотрудничества в рамках ФАТФ; наладить международный информационный обмен между криптобиржами и другими операторами криптовалютного рынка.

---

[1] URL: https://www.justice.gov/usao-wdwa/pr/former-microsoft-software-engineer-sentenced-nine-years-prison-stealing-more-10-million (дата обращения: 12.11.2020)

С.В. Кондратюк,
старший преподаватель кафедры
«Уголовное право и процесс»
Тольяттинского государственного
университета

Информационные источники следственной и судебной профилактики преступного занятия высшего положения в преступной иерархии

Организованная профессиональная преступность признается одним из наиболее общественно опасных видов преступной деятельности. Стратегия национальной безопасности Российской Федерации определяет организованную преступность как угрозу национальным интересам и конституционному строю государства. Главенствующая роль в среде профессиональных преступников принадлежит статусным лидерам преступного сообщества – ворам в законе. Деятельность таких верховных лидеров преступного сообщества направлена на формирование идеологии преступного мира, закрепление и воспроизводство его принципов и обычаев в социуме[1]. Вызывает озабоченность информационная деятельность преступных идеологов, направленная на управление противозаконной деятельностью лиц, придерживающихся идеологии воровского мира, а также на наращивание политического влияния и использование его в своих псевдодуховных и квазиморальных целях[2]. Для задач распространения влияния криминальной среды статусные лидеры преступного сообщества используют информационное пространство социальных сетей. Так, информационной поддержкой сопровождается процедура признания новых лиц статусными лидерами преступного сообщества.

В ходе профилактики преступного занятия высшего положения в преступной иерархии следственные и судебные органы опираются на конкретные признаки состава указанного преступ-

---

[1] *Сенатов А.В.* Трансформация традиций криминальной субкультуры в отношении лидеров уголовно-преступной среды // Пенитенциарное право: юридическая теория и правоприменительная практика. 2020. № 3 (25).

[2] *Величко Ф.М., Копылов В.В., Субботин А.А.* Проблемы противодействия организованной преступности в РФ // Вестн. экон. безопасности. 2020. № 1.

ления[1]. Элементы состава преступления находят отражение в информационном пространстве социума. Однако до настоящего времени в научной литературе не рассмотрены вопросы применения информационных источников в следственной и судебной профилактике преступлений указанного вида.

Вопросы профилактической деятельности органов досудебного следствия и суда исследованы в работах Р.С. Белкина, В.К. Гавло, Г.И. Грамовича, А.В. Дулова, И.И. Иванова, А.М. Кустова, И.П. Лопушанского, С.А. Шейфера, М.Ш. Махтаева, Н.П. Яблокова и других ученых. В соответствии со ст. 73 УПК РФ в процессе производства по уголовному делу установлению подлежат причины и условия, способствовавшие совершению преступления. При выявлении обстоятельств профилактического характера суд выносит по ним частное определение (ст. 29 УПК РФ).

Объективная сторона преступления определена внешней стороной общественно опасного посягательства на отношения, сложившиеся в социуме. В рассматриваемом случае объективная сторона преступного занятия высшего положения в преступной иерархии отображает внешние признаки действий лица, стремящегося его занять. Так, для характеристики объективной стороны преступления важное значение приобретает способ его совершения. В уголовно-правовой науке способ совершения преступления трактуют как систему поведенческих актов, применяемых лицом при совершении преступления[2]. Авторы под способом совершения преступления понимают последовательность конкретных действий, приемов и способов для достижения субъектом преступления поставленной цели. Очевидно, что способ совершения преступления содержит признаки поставленной преступной цели. По поводу преступного лидерства можно констатировать наличие в нем специфических действий лица-претендента на высший статус в преступной иерархии и его соучастников. С точки зрения технологического подхода, способ совершения преступления детерминирует рабочие операции по достижению же-

---

[1] *Герасимова Е.В., Ченчиковский А.Д.* Организованная преступность. Высшее положение в преступной иерархии: уголовный закон, его толкование и применение // Вестн. Волж. ун-та им. В.Н. Татищева. 2020. Т. 1. № 2 (95).

[2] *Бондаренко С.В.* Влияние так называемых «воров в законе» на криминологическую ситуацию в пенитенциарных учреждениях // Вестн. Самар. юрид. ин-та. 2020. № 2 (38).

лаемой цели. В настоящее время большинство ученых определяют способ совершения преступления как метод, порядок и последовательность действий, применяемых лицом при совершении преступлений[1]. Поэтому в результатах действий по достижению лидерского положения в преступной иерархии могут быть отображены признаки способа данного преступления.

Рассмотрим каналы отображения в информационных сетях элементов способа преступного занятия высшего положения в преступной иерархии.

Способ совершения рассматриваемого преступления распределяем на этапы последовательного достижения преступного результата. На этапе выдвижения нового кандидата в статусные лидеры преступного сообщества уже признанные преступным сообществом статусные лидеры производят обсуждение отобранных кандидатур на присвоение высшего положения в преступной иерархии. Отбор указанного кандидата ведется среди активных участников преступного сообщества, доказавших свою приверженность к преступной идеологии. Возможность осуществления данной процедуры может свидетельствовать, что в определенном социуме на занимаемой им территории уже сложилось сообщество, опирающееся в своей деятельности на преступные обычаи, традиции, другие принципы криминального мировоззрения. Из этого можно заключить, что распространение преступной идеологии в социуме стало необходимым условием реализации объективной стороны преступного занятия лицом лидерского положения в преступной иерархии. На современном этапе средствами распространения преступной идеологии служат социальные сети, поэтому профилактической задачей следственных и судебных органов становится выявление и фиксация информационных каналов распространения преступной идеологии и ведения пропаганды криминального мировоззрения.

Действия статусных лидеров по подбору кандидата на статус нового преступного лидера предполагают их активное участие в преступной деятельности с целью демонстрации собствен-

---

[1] *Кутякин С.А., Теткин Д.В., Брюхнов А.А.* От «бродяг» и «Иванов» к «ворам в законе»: история и современные перспективы противодействия криминальному феномену // Философия права. 2020. № 3 (94).

ной приверженности к идеям преступного мира. Также деятельность преступных лидеров содержит активное обсуждение предлагаемых кандидатур. Оба направления действий преступных лидеров неизбежно отображаются техническими средствами социальной коммуникации[1]. Профилактическое значение приобретает установление отобразившихся в коммуникативных сетях фактов активных действий статусных лидеров преступного сообщества, а также фактов обсуждения кандидатур на присвоение статуса преступного лидера.

Этапом реализации способа совершения рассматриваемого преступления называем организацию и проведение воровской сходки. По сравнению с предыдущим этапом здесь дополнительно участвуют лица обеспечивающего персонала – технические помощники статусных лидеров по организации воровской сходки, а также лица, осуществляющие охрану данного мероприятия, техники связи и др.[2] Очевидно, что все они становятся как адресантами, так и адресатами передачи информационных сообщений о ходе подготовки и реализации преступной цели. Обращаем внимание, что указанные лица представляют собой точки выхода и входа в информационных каналах передачи сведений о рассматриваемом преступлении. По данным авторов, при этом широко используются защищенные каналы связи. В любом случае профилактическое значение в ходе расследования и судебного рассмотрения дел данной категории приобретает отслеживание информационных потоков указанного характера и содержания.

На завершающем этапе реализации способа рассматриваемого преступления информация о назначении нового преступного лидера должна быть доведена да широкого круга заинтересованных лиц[3]. В него входят в первую очередь статусные лидеры и другие участники преступного сообщества. Преступ-

---

[1] *Гришко А.Я.* Уголовная ответственность лидеров преступного мира: вопросы реализации // Вестн. Уфим. юрид. ин-та МВД России. 2020. № 1 (87).

[2] *Бабушкин А.А., Белянский Е.Б.* Организационно-правовые основы оперативно-разыскного контроля за лицами, занимающими высшее положение в преступной иерархии // Вестн. Волгоград. акад. МВД России. 2020. № 1 (52).

[3] *Шутемова Т.В.* Об изучении личности преступника // Вектор науки Тольяттинского гос. ун-та. Сер.: Юрид. науки. 2017. № 4 (31).

ные лидеры информируют заинтересованных представителей власти, бизнеса, общественных организаций о назначении нового статусного лидера. С целью укрепления и распространения влияния преступной идеологии эти сведения проникают и в общедоступную информационную среду. Информация подобного содержания также может быть использована следственными и судебными органами для выработки рекомендаций профилактического характера.

Обратим внимание на субъективную сторону и субъекта преступного занятия лидерского положения в преступной иерархии. Можно утверждать, что кандидат на лидерский статус в преступном сообществе сознательно стремится его получить. Выполняемые им действия по пропаганде собственной кандидатуры и распространению преступной идеологии носят целенаправленный и системный характер. Что касается субъекта преступления, то его личностные характеристики должны соответствовать принципам, закрепленным в преступной среде[1]. Поэтому профилактические рекомендации следствия (суда) должны касаться и лиц, активно поддерживающих традиции криминального мира.

Выводы. Предложено использовать коммуникативные сети в качестве информационных источников следственной и судебной профилактики преступного занятия высшего положения в преступной иерархии.

Показан механизм отображения элементов состава рассматриваемого преступления информационными средствами в социальных сетях и на других интернет-ресурсах.

Рекомендовано следственным (судебным) органам в ходе досудебного следствия (судебного рассмотрения) преступления данного вида устанавливать обстоятельства профилактического характера путем выявления информационных источников об элементах способа его совершения.

Конкретизированы информационные источники, отображающие обстоятельства, способствовавшие реализации объективной стороны данного преступления: факты, отображающие дея-

---

[1] *Кутякин С.А.* Влияние «воров в законе» на криминологическую ситуацию в исправительных учреждениях // Уголовно-исполнит. право. 2014. № 2 (18).

тельность статусных лидеров преступного сообщества; обстоятельства выдвижения лица на высшее положение в преступной иерархии; условия подготовки и проведения воровской сходки, на которой принимается решение о присвоении лицу лидерского статуса в преступной иерархии; обстоятельства, способствовавшие широкому распространению сведений о признании нового лица лидером преступной иерархии.

Обстоятельства, определяющие субъект данного преступления, отражены в личностных характеристиках лица, занимающего высшее положение в преступной иерархии. К профилактическим мерам относим установление фактов распространения криминальной идеологии информационными ресурсами. Профилактическое значение приобретает и выявление лиц, стремящихся занять высшее положение в преступной иерархии.

А.Л. Коренюк,
старший научный сотрудник
Университета прокуратуры
Российской Федерации

Современное состояние и тенденции учета преступлений в сфере компьютерной информации

На современном этапе развития общественных отношений, когда человеческая жизнь пронизана информационными технологиями, уже невозможно обходиться без них в повседневной жизни. В то же время защитить информацию сложно. Рост количества киберпреступлений становится пропорциональным технологическому прогрессу, при этом они принимают все более разнообразные формы, посягая на различные объекты уголовно-правовой охраны: от жизни и здоровья граждан до общественной нравственности и интересов государственного строя.

В многочисленных источниках отмечается о возрастающих темпах роста количества рассматриваемых преступлений. Согласно официальными статистическим данным, в период с января по декабрь 2020 г. на территории Российской Федерации было заре-

гистрировано свыше 510 тыс. компьютерных преступлений. Данный показатель по сравнению с 2019 г. (свыше 294 тыс.) вырос на 73,4%. Более 50% всех компьютерных преступлений было совершено с использованием сети «Интернет», средства мобильной связи использовались злоумышленниками в 33% случаев[1]. Несмотря на принимаемые меры, за 2020 г. увеличилось число преступлений, совершенных с использованием IT-технологий. В частности, количество краж возросло на 75,5%, противоправных деяний, предусмотренных ст. 159, 159^3, 159^6 УК РФ, – на 76,1%[2].

Анализируя степень тяжести преступлений, совершаемых с использованием компьютерных технологий, следует отметить, что чуть менее половины из них составляют преступления, подпадающие под категорию тяжких и особо тяжких (48,7%), при этом удельный вес преступлений, совершаемых с использованием сети «Интернет», составил 52,6%, свыше трети всех совершенных в анализируемый период преступлений совершены с помощью средств мобильной связи (38,5%).

В подавляющем большинстве компьютерные преступления совершаются путем хищения в форме кражи или мошенничества. Доля таких преступлений составляет 79% от их общего числа. На втором месте по распространенности преступления, связанные с незаконным оборотом наркотических средств, психотропных веществ, их аналогов, а также оружия и порнографических материалов (8,6%).

Одним из наиболее значимых инструментов, необходимых для повышения качества и результативности анализа компьютерной преступности, является учет статистических показателей.

Для обобщения статистической информации о компьютерных преступлениях в нашей стране до 2018 г. использовалась форма статистической отчетности № 1-ВТ, утвержденная приказом МВД России от 01.04.2002 № 31, в соответствии с которой правоохранительные органы вносили показатели, характеризую-

---

[1] Данные приведены из формы № 4-ЕГС «Сведения о состоянии преступности и результатах расследования преступлений» за январь – декабрь 2019 г. (дата обращения: 18.01.2021).

[2] Данные приведены из формы № 4-ЕГС «Сведения о состоянии преступности и результатах расследования преступлений» за январь – декабрь 2020 г. (дата обращения: 18.01.2021).

щие объективные признаки преступлений, а также уголовно-процессуальные аспекты, касающиеся их выявления, раскрытия и расследования.

Оценка показателей статистического отчета по форме № 1-ВТ приводит к выводу о том, что данная форма не являлась всеобъемлющей, поскольку термин «компьютерные преступления» использовался в ней в узком смысле. В отчет были включены 10 составов преступлений (ст. 158, 159, 159^3, 159^6, 183, 272–274 УК РФ), а деяния, не подпадающие под критерии ни одного из разделов, отмечались в разделе «иные преступления». О необходимости корректировки указанного отчета неоднократно отмечалось в различных криминологических исследованиях[1].

Однако законодатель учел обозначенную необходимость частично, включив в 2016 г. в форму отчета отдельные виды мошенничества, ответственность за которые предусмотрена ст. 159^3, 159^6 УК РФ. Тем не менее структура отчета по форме № 1-ВТ фактически не позволяла учитывать каждое пятое преступление, совершенное с использованием компьютерных технологий, а также разрабатывать методические рекомендации по раскрытию и расследованию данных преступлений, фиксации следов преступления, имеющих доказательственное значение, вырабатывать концептуальные основы профилактики киберпреступности.

Активное использование информационно-коммуникационных технологий в преступной деятельности способствовало пересмотру правоохранительными органами подходов к учету компьютерных преступлений. Поэтому информация о данных преступлениях с января 2018 г. стала предоставляться ежемесячно по форме статистической отчетности № 4-ЕГС, введенной приказом Генерального прокурора Российской Федерации от 28.08.2017 № 592. В первоначальной редакции раздела 11 указанного отчета было предусмотрено 33 состава преступлений, совершаемых с использованием информационно-коммуникационных технологий, где к ранее учитываемым преступлениям добавились предусмотренные ст. 110, 110^1, 137, 138, 138^1, 146, 151, 151^2, 163, 165, 171^2, 172^2, 185^3, 187, 205^2,

---

[1] *Соловьев В.С.* Преступность в социальных сетях Интернета (криминологическое исследование по материалам судебной практики) // Криминолог. журн. БГУЭП. 2016. Т. 10. № 1. С. 71.

222, 222^1, 228^1, 228^2, 228^4, 230, 234, 242, 242^1 242^2, 280, 280^1, 282 УК РФ. В 2020 г. в данную форму были добавлены составы преступлений, предусмотренные ст. 135, п. «г» ч. 3 ст. 158, ч. 1 ст. 258^1, п. «б» ч. 2 ст. 258^1, ст. 274^1 УК РФ[1].

Таким образом, в обновленную форму статистической отчетности по компьютерным преступлениям необходимо было включение не только «классических» составов, но и иных преступлений, при которых виновный реализует свой преступный умысел с использованием технологий сети «Интернет» (социальные сети, мессенджеры, площадки для электронной коммерции, платформы для торговли цифровыми финансовыми активами и т.д.).

Основным препятствием, стоящим перед субъектами статистического учета преступлений в сфере компьютерной информации, является системная латентность (гиперлатентность) указанной категории преступлений. Дело в том, что компьютерная преступность практически не поддается внятному количественному измерению, поскольку имеет комплексный характер. Помимо указанного несовершенства механизмов статистического учета, к числу причин гиперлатентности компьютерных преступлений следует отнести противоречия нормативного регулирования, несовершенство правоприменительной деятельности, массовые случаи несообщения о причинении вреда потерпевшими, а также постоянно видоизменяющаяся природа цифровой преступности. По оценкам специалистов, 85–97% компьютерных преступлений не обнаруживается[2]. Тезис о латентности рассматриваемой категории преступлений подтверждается и практикующими адвокатами в области киберправа. Так, в последнее время частыми являются случаи взлома аккаунтов пользователей игровых сервисов с целью хищения артефактов (например, танк в онлайн-игре World of Tanks), стоимость которых может превышать десятки тысяч долларов. Между тем граждане, подвергающиеся преступным посягательствам такого рода, как правило, предпочитают не

---

[1] Приказ Генерального прокурора РФ от 17.01.2020 № 30 «Об утверждении формы федерального статистического наблюдения № 4-ЕГС «Сведения о состоянии преступности и результатах расследования преступлений».

[2] См.: *Противодействие* киберпреступности в аспекте обеспечения национальной безопасности: монография / [П.В. Агапов и др.]. М., 2014. С. 35.

обращаться в правоохранительные органы, поскольку уверены в бессилии последних в данных вопросах[1].

В современных научных работах латентность рассматривается как внутреннее репродуктивное свойство (внутренний источник самовоспроизводства) преступности[2], что отсылает нас к его особому признаку – мультипликативности.

У.В. Зинина небезосновательно делает вывод о том, что в официальную статистику преступности в сфере компьютерной информации включаются случаи не вполне корректного применения правоприменительными органами уголовного закона, свидетельствующие о расширительном толковании элементов состава преступления, предусмотренного ст. 272 УК РФ[3]. В защиту подобной практики следует лишь сослаться на то, что такое положение во многом обусловлено несовершенством нормативной базы.

Вместе с тем полагаем, что даже обновленная форма статистической отчетности о компьютерных преступлениях неполно отражает реальную криминогенную обстановку.

Не случайно с целью повышения эффективности деятельности правоохранительных органов и минимизации фактов сокрытия информации о совершенных преступлениях принят Федеральный закон от 27.12.2019 № 487-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам государственного единого статистического учета данных о состоянии преступности, а также о сообщениях о преступлениях, следственной работе, дознании, прокурорском надзоре», в соответствии с которым основным субъектом, координирующим деятельность по обобщению статистических сведений о состоянии преступности на территории Российской Федерации, является Генеральная прокуратура Российской Фе-

---

[1] *Киберпреступлений* становится все больше, однако их раскрываемость уменьшается. Генеральная прокуратура предоставила «АГ» расширенную статистику преступлений, совершаемых с использованием современных технологий. URL: https://www.advgazeta.ru/novosti/kiberprestupleniy-stanovitsya-vse-bolshe-odnako-ikh-raskryvaemost-umenshaetsya/ (дата обращения: 17.01.2021).

[2] См., например: *Макаров В.В.* Криминологическое исследование самодетерминации преступности: автореф. дис. … канд. юрид. наук. М., 2014. С. 8.

[3] *Зинина У.В.* Преступления в сфере компьютерной информации в российском и зарубежном уголовном праве: автореф. дис. … канд. юрид. наук. М., 2007. С. 23.

дерации. Полномочия по утверждению форм статистической отчетности, обеспечению функционирования государственной автоматизированной системы правовой статистики (ГАС ПС)[1] также переданы Генеральной прокуратуре Российской Федерации.

Все материалы официально опубликованной статистики, имеющейся в Российской Федерации, обобщаются на основе специальных статистических карточек, заполняемых сотрудниками правоохранительных органов и работниками судебной системы. Значимость данных статистических карточек состоит в том, что в них дается разносторонняя характеристика каждого преступления, подлежащего учету. Данная информация имеет особое значение для правоохранительных органов при прогнозировании преступности и выявлении основных криминологических тенденций. Достоверность и полнота сведений, заносимых в статистические карточки, влияют на оценку эффективности правоохранительной деятельности.

Одним из наиболее криминологически значимых свойств преступления, существенно повышающим его общественную опасность, является серийность. Поэтому для целей криминалистики и криминологии необходим учет статистической информации не только по количеству и объективным признакам совершенного преступления, но и по признакам, позволяющим идентифицировать информацию о механизмах и способах совершения компьютерных преступлений, что требует особых знаний и навыков от субъектов данного учета. Однако к настоящему времени такие показатели не учитываются в статистических формах. Поэтому представляется целесообразным установление в статистических карточках по уголовным делам, заполняемых органами предварительного расследования и судами, закрепление особого реквизита «совершено с использованием сети «Интернет».

---

[1] Использование ГАС ПС на постоянной основе должно изменить устаревшие способы обработки статистической информации посредством введения унифицированных форматов сбора данных, обеспечить интеграцию информационных ресурсов, используемых в сфере борьбы с преступностью. На начало 2019 г. в ГАС ПС были учтены 1,4 млн преступлений, более 1 млн потерпевших, 909,5 тыс. подозреваемых (обвиняемых), а также 16,9 млн сообщений о преступлениях.

Дополнительным преимуществом обновленных форм статистического учета (при условии их взаимной интеграции с системами криминалистического учета, функционирующими в настоящее время) является возможность привязки конкретного лица к нескольким эпизодам преступной деятельности с использованием компьютерных технологий, квалифицируемым по различным нормам Уголовного кодекса Российской Федерации.

Более того, детализация показателей статистической отчетности может способствовать раскрытию нескольких эпизодов, объединению уголовных дел по преступлениям, совершенным на территории разных субъектов, в одно производство, а также достижению иных целей. Например, в различных субъектах Российской Федерации в рамках расследования уголовного дела по факту распространения в социальной сети лицом порнографических либо экстремистских материалов, скачанных из интернет-ресурса, может быть выделено (возбуждено) уголовное дело по факту изготовления идентичных материалов и их размещения на одном и том же интернет-сайте.

В ходе анализа обобщена информации о сложившейся системе учета статистических показателей компьютерной преступности в Российской Федерации, за последние два года выявлена тенденция к их увеличению. Отмечается ряд особенностей данного вида преступлений, которые совершаются, как правило, лицами, имеющими высокую профессиональную квалификацию, с использованием интеллектуальных средств и орудий преступления. Данные преступления отличаются высокой латентностью, низкой раскрываемостью. Для их расследования необходимы высококвалифицированные специалисты и соответствующие аппаратные и программные средства. Также отмечается важность инструментария статистического учета информации для исследований в области наук уголовно-правового цикла с целью предупреждения и раскрытия преступлений.

В рамках проведенного сравнительного анализа форм статистической отчетности, существовавших в России с 2002 г. по настоящее время, определены их преимущества и недостатки.

Вместе с тем можно утверждать, что сформирован инструментарий для обобщения и анализа информации о компьютерных преступлениях. Назвать его полноценным сегодня пока не представляется возможным. Полагаем, что работа по оптимизации форм статистической отчетности анализируемых преступлений – это динамический процесс, требующий постоянного внимания со стороны законодателя и правоохранительных органов. Кроме того, считаем необходимой более выраженную структурную интеграцию статистической отчетности по форме № 4-ЕГС с автоматизированными системами криминалистического учета правоохранительных органов. Также на уровне правоохранительных органов и ведомственных образовательных организаций целесообразно регулярно предпринимать меры по выработке единого подхода к категоризации преступлений, в которых используются информационные технологии. Категоризацию необходимо учитывать в системе регистрации и учета компьютерных преступлений. Это позволит более качественно проводить работу по выявлению, раскрытию и расследованию компьютерных преступлений и может упростить решение задач, стоящих перед правоохранительными органами.

Э.Т. Халиуллина,
старший научный сотрудник
НИИ Университета прокуратуры
Российской Федерации

Основные проблемы противодействия преступлениям, совершаемым с использованием персональных данных, и пути их решения

В последнее время вопросы обеспечения безопасности персональных данных заслуживают пристального внимания, поскольку являются особым объектом организационно-правовой защиты. Человек, выступая в роли субъекта многих правовых отношений, оказывается особо уязвимым в информационном пространстве, поскольку реализация его прав и свобод связана с ис-

пользованием частной информации о нем, т.е. персональных данных[1].

Совет Безопасности Российской Федерации также отмечает, что государство в информационной сфере подвергается множеству угроз. Так, при обработке персональных данных с использованием информационно-телекоммуникационных систем увеличивается число преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина, в частности затрагивающих не только неприкосновенность частной жизни, но и личную и семейную тайну[2]. Ярким доказательством этого являются новостные ленты средств массовой информации, в том числе информация, размещаемая на сайтах правоохранительных, надзорных и контролирующих органов, о состоянии правонарушаемости и преступности в области защиты прав субъектов персональных данных.

Таким образом, активно возрастающая угроза атак на персональные данные человека свидетельствует о том, что защита персональных данных – это одна из злободневных проблем современного мира[3].

Анализ состояния преступности свидетельствует об увеличении числа различного рода утечек персональной информации. Наблюдается существенный рост противоправных посягательств в отношении персональной информации, а также незаконного использования личной информации при совершении различных преступных действий. Факты неправомерного распространения персональных данных встречаются в правоприменительной деятельности как органов государственной власти, так и негосударственных структур, наделенных правом доступа к информации частного характера. Неправомерное распространение персональных данных нередко совершается специальными субъектами –

---

[1] *Макаров А.В., Вологдина Е.С.* Персональные данные как объект преступных посягательств на неприкосновенность частной жизни: законодательный опыт в России и зарубежных странах // Рос. следователь. 2019. № 5.

[2] Доктрина информационной безопасности Российской Федерации, утв. Указом Президента РФ от 05.12.2016 № 646.

[3] *Шумекеева Г.Б.* Защита персональных данных как одна из проблем современного мира // Право: современные тенденции : материалы VI Междунар. науч. конф. (г. Краснодар, окт. 2018 г.). Краснодар : Новация, 2018.

должностными лицами либо государственными служащими, использующими свое служебное положение. Поэтому актуальной становится проблема антикоррупционной надежности персонала и обеспечения надлежащего механизма правовой защиты личной информации.

По мнению экспертов[1], на преступность данного вида влияют следующие социальные и экономические факторы:

компьютеризация российского общества – 47,5% (±3,8%);

низкий уровень правовой грамотности населения – 43,4 % (±3,8%);

переход на безналичные расчеты – 34,0% (±3,6%);

виктимилогические факторы совершения таких преступлений – 18,3% (±3,0%);

низкий уровень жизни, безработица – 13,5% (±2,6%).

Как отмечают исследователи[2], несмотря на массовое использование сети «Интернет», для большинства россиян при этом угроза столкновения с противоправными действиями в этой реальности носит гипотетический характер. Вместе с тем граждане высказывают достаточно высокий уровень тревожности относительно возможного использования персональных данных.

Таким образом, приоритетные задачи должны быть направлены на рост цифровой грамотности населения через образовательные программы и инициативы для разных возрастных категорий граждан и на создание сервисов для пользователя, позволяющих оперативно проследить за всеми соглашениями об обработке личных данных, которые гражданин дал различным компаниям.

В связи с этим актуальной и своевременной является инициатива Роскомнадзора о необходимости знаний правил информационной безопасности в сети «Интернет» несовершеннолетней

---

[1] В 2020 г. в Университете прокуратуры Российской Федерации проведено исследование на тему «Деятельность прокуратуры по профилактике преступлений, совершаемых с использованием персональных данных». Для анализа криминальной ситуации в рассматриваемой сфере по специально разработанным анкетам о состоянии и проблемах противодействия преступности данной категории был опрошен 661 работник органов прокуратуры. Анкетирование проведено среди слушателей факультета профессиональной переподготовки и повышения квалификации Университета прокуратуры Российской Федерации и в прокуратурах субъектов Российской Федерации.

[2] URL: https://news.myseldon.com/ru/news/index/197926905 (дата обращения: 25.12.2020).

аудитории. Как отмечают эксперты, дети и подростки являются самой уязвимой частью интернет-сообщества – ими проще манипулировать, чем активно пользуются злоумышленники[1].

Отметим, что прокурорские работники, указывая на встречающиеся в ходе надзорных мероприятий по защите прав субъектов персональных данных проблемы, в первую очередь выделили:

несоблюдение требований по обеспечению конфиденциальности персональных данных;

несовершенство законодательства, регулирующего вопросы обеспечения защиты персональных данных;

отсутствие должного взаимодействия контролирующих и правоохранительных органов;

недостатки в деятельности контролирующих органов.

Известны случаи, когда преступные посягательства в отношении личной информации не всегда могут быть правильно квалифицированы. Проблемным становится вопрос реализации норм, регулирующих общественные отношения в сфере охраны персональных данных граждан. Это связано с тем, что нормы уголовного права не в полной мере учитывают специфику активно развивающегося института персональных данных и видов преступлений, установленных Уголовным кодексом Российской Федерации.

В связи с этим актуальным является предложение практических работников (прокуратура Нижегородской области) о том, что с учетом роста преступлений данного вида в целях повышения эффективности работы и совершенствования уголовного законодательства целесообразно включение квалифицирующего признака преступления «с использованием персональных данных иных лиц» в ст. 158 и 159, а также ряд других статей УК РФ. Почти каждый третий прокурорский работник из принявших участие в анкетировании предложил ввести новый состав преступления, предусматривающий ответственность за противоправные действия в сфере оборота и защиты персональных данных граждан. При этом, например, отягчающими обстоятельствами данного состава могло бы быть совершение противоправного деяния с

[1] URL: https://vm.ru/news/634049-ekspert-problema-zashity-personalnyh-dannyh-nabiraet-aktualnost-s-kazhdym-dnem (дата обращения: 25.12.2020).

персональными данными с использованием служебного положения либо с наступлением особо тяжких последствий (гибель или причинение тяжкого вреда здоровью субъекта персональных данных).

Высказывая предложения по совершенствованию уголовного законодательства, прокуроры также выступили за:

включение квалифицирующего признака преступления «совершение с использованием персональных данных» в ряд других составов УК РФ;

ужесточение санкций за совершение преступлений данного вида;

включение в ст. 63 УК РФ нового обстоятельства, отягчающего наказание, – «с использованием персональных данных» (в случаях, когда соответствующий признак не включен в конкретный состав в качестве квалифицирующего).

Учитывая, что сегодня сеть «Интернет» является одним из главных средств свободного распространения информации, аккумулирующим практически все доступные источники информации, возникает необходимость правового регулирования данной сферы. С одной стороны, обеспечиваемые ст. 29 Конституции Российской Федерации свобода слова, свобода получения, использования и распространения информации любым законным способом не подлежат ни ограничению, ни ущемлению. Однако, с другой стороны, в целях обеспечения прав граждан очевидна необходимость защиты персональных данных граждан, права на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и достоинства[1].

Для обеспечения конституционных прав и свобод человека и гражданина при обработке персональных данных, по мнению опрашиваемых, необходимо отнести уголовные дела о преступлениях, предусмотренных ч. 1 ст. 137 УК РФ, к числу дел публичного обвинения (путем внесения изменений в ч. 3 ст. 20 УПК РФ) – 37,5 % (±3,7%). Кроме того, целесообразно изменить систему учета преступлений, совершаемых с использованием персональных данных (внесение корректив в статистические кар-

[1] *Гундерич Г.А.* Проблема защиты персональных данных // Науч. вестн. Крыма. 2017. № 5 (10).

точки первичного учета преступлений и формы федерального статистического наблюдения) – 28,6% (±3,4%).

По-прежнему одной из основных проблем, возникающих в ходе профилактики преступлений, совершаемых с использованием персональных данных, является ненадлежащая организация взаимодействия на региональном и межрегиональном уровнях правоохранительных органов с кредитно-финансовыми организациями, операторами сотовой связи, поставщиками интернет-услуг. Данный аспект проблемы должен быть в поле зрения надзорной практики прокуроров.

В целях совершенствования работы по профилактике указанных преступлений и активизации надзора прокурорам субъектов Российской Федерации необходимо регулярно проводить работу не только по правовому просвещению, но и по информированию нижестоящих прокуроров о состоянии законности в сфере исполнения законодательства о персональных данных, в том числе несовершеннолетних, об изменениях федерального законодательства в области защиты прав субъектов персональных данных, о результатах надзорной деятельности и судебной практике по вопросам привлечения к административной ответственности за рассматриваемые правонарушения, распространять положительный опыт работы.

На основании проведенного исследования можно выделить несколько групп проблем в сфере защиты персональных данных: правовые, организационные и финансовые; проблемы, связанные с защитой и оборотом персональных данных; защиты тайны личной жизни при условии свободы слова в средствах массовой информации.

Кроме того, к проблемам противодействия преступлениям, совершаемым с использованием персональных данных, можно отнести отсутствие в Уголовном кодексе Российской Федерации специального состава преступления в сфере оборота и защиты персональных данных.

Таким образом, перечисленные проблемы свидетельствуют о том, что действующее законодательство нуждается в существенной доработке. Государство обязано совершенствовать правовое регулирование в области обработки и защиты персональ-

ных данных, а также усилить контроль за деятельностью лиц и организаций, которые вправе совершать операции с таким видом информации[1].

Важной проблемой осуществления прокурорами профилактики рассматриваемых преступлений является также повышение эффективности виктимологического ее аспекта. Основной его смысл сводится к тому, что сами граждане должны принимать меры к обеспечению безопасности своих персональных данных. Тесное взаимодействие государства и граждан, повышение уровня правовой грамотности населения позволят качественно усовершенствовать действующее законодательство и успешно решить имеющиеся в профилактической деятельности прокуроров проблемы.

П.А. Россоловский,
соискатель Санкт-Петербургского
юридического института (филиала)
Университета прокуратуры
Российской Федерации

Некоторые вопросы применения информационно-коммуникационных технологий в органах прокуратуры в контексте организации работы и управления

Современные социально-экономические условия определяют новый взгляд на вопросы, связанные с применением информационно-коммуникационных технологий в органах и организациях прокуратуры.

В условиях проведения реформирования законодательства существенное значение приобретают отдельные вопросы внедрения в органы прокуратуры различных автоматизированных систем и их практического применения.

[1] *Крюкова Д.Ю., Мокрецов Ю.В.* Актуальные проблемы правового регулирования оборота и защиты персональных данных в России // Пенитенциарная наука. 2017. № 2 (38).

Современные информационные технологии становятся неотъемлемой частью повседневной жизни и управленческих процессов органов и организаций прокуратуры. Проблема развития навыков у прокурорских работников в части работы с цифровыми технологиями также актуальна.

В рамках совместного проекта с Генеральной прокуратурой Российской Федерации Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации выступает технологическим экспертом внедряемых решений цифровой трансформации органов и организаций прокуратуры с использованием цифровых платформ координации органов правопорядка и органов контроля и надзора[1].

Мероприятия по цифровой трансформации органов и организаций прокуратуры включены в федеральный проект «Цифровое государственное управление» национальной программы «Цифровая экономика Российской Федерации» и направлены на обеспечение высокотехнологичного надзора в деятельности органов прокуратуры, координацию правоохранительных органов Российской Федерации с использованием цифровых технологий, а также функционирование современных автоматизированных рабочих мест и сервисов работы с цифровыми данными на базе защищенной цифровой инфраструктуры Генеральной прокуратуры Российской Федерации.

В настоящее время мероприятия, предусмотренные Концепцией цифровой трансформации органов и организаций прокуратуры и частично реализованные, – широко обсуждаемая тема как среди ученых, так и среди практических работников органов прокуратуры. Отдельные вопросы и проблемы внедрения в органы прокуратуры различных автоматизированных систем рассматриваются и как теоретические положения, что позволяет сделать вывод о том, что данному вопросу в дальнейшем будет придаваться научное осмысление и теоретическое обеспечение[2].

---

[1] *Цифровая* трансформация органов и организаций прокуратуры Российской Федерации. URL: https://digital.gov.ru/ru/activity/directions/842/ (дата обращения: 18.01.2021).

[2] *Реализация* Концепции цифровой трансформации органов и организаций прокуратуры в современных условиях: сб. материалов круглого стола (Москва, 11 июня 2019 г.) / под общ. ред. Е.Ю. Лихачевой; Ун-т прокуратуры Рос. Федерации. М., 2019. С. 4–5.

Применительно к вопросам организации работы и управления в органах прокуратуры Российской Федерации важно отметить, что создание оптимальных условий взаимодействия органов, подразделений и должностных лиц для достижения целей функциональной деятельности органов прокуратуры возможно с использованием информационного обеспечения и применения информационно-коммуникационных технологий.

Организация работы является сложным видом деятельности, основным содержанием которой является упорядочение, налаживание эффективного функционирования системы органов прокуратуры. В конечном итоге эта деятельность направлена на создание эффективной системы и структуры управления.

По мнению Е.Ю. Лихачёвой, «управление в органах прокуратуры состоит из системы организационных, правовых, социально-психологических, нравственных мероприятий, выполняемых конкретными уполномоченными прокурорами, направленных на обеспечение эффективного использования знаний и навыков работников как в интересах структурного подразделения органа прокуратуры, так и в интересах прокуратуры Российской Федерации в целом»[1].

Важно отметить, что взаимодействие является основным вопросом, отражающим содержание организации работы в органах прокуратуры, а управление в системе органов прокуратуры Российской Федерации, в свою очередь, представлено системой специфических действий и операций «направляющего свойства».

Согласимся с мнением В.В. Стрельникова, который организационные аспекты, связанные с обеспечением деятельности прокурорских работников, выводит на первый план. При этом, по его мнению, общая задача повышения действенности управления в органах прокуратуры решается многообразно: разрабатываются и осуществляются меры, нацеленные на повышение уровня руководства надзорной деятельностью, совершенствование организа-

[1] *Лихачёва Е.Ю.* Цифровизация меняет организационно-управленческие функции в органах прокуратуры // Законность, 2020. № 7.

ционного построения, информационно-аналитической работы, планирования, контроля и иных видов и форм управления[1].

Создание единой информационной среды, развитие коммуникации в системе, а также между органами прокуратуры и гражданами, свобода доступа к информации, возможность создания баз данных и организация работы с большим количеством информации, ее анализ способствуют совершенствованию и повышению эффективности путем улучшения организационной стороны.

Видится, что некоторое применение информационно-коммуникационных технологий в органах прокуратуры в рамках организации работы и управления с точки зрения практической реализации будет способствовать совершенствованию механизма надзорной деятельности, наращиванию положительной практики и созданию эффективной управленческой модели в органах прокуратуры.

Вместе с тем в числе новшеств, предлагаемых цифровой трансформацией, можно назвать упрощение процесса подачи обращения в органы прокуратуры, существенное сокращение срока его прохождения за счет использования электронного документооборота. Также предусмотрена возможность подачи обращения и записи на прием в органы прокуратуры через портал государственных услуг. Таким образом, органы прокуратуры действительно становятся ближе к обществу, а роль прокурорских работников в устранении различных нарушений закона только возрастает.

Важно отметить, что совершенствование информационного обеспечения органов прокуратуры способствует решению таких вопросов организации работы, как определение количества входящих в создаваемую организационную систему органов, подразделений, должностных лиц, установление между ними взаимосвязи, определение целей и задач их деятельности, функций, полномочий, определение системы взаимодействия, организация контроля и исполнения, оценка возможностей использования ре-

[1] *Стрельников В.В.* Понятие и содержание управленческой деятельности в органах отечественной прокуратуры // Советник юриста. 2012. № 2. С. 26.

сурсов и их обеспечение, рациональное управление документацией.

Немаловажны в работе органов и организаций прокуратуры открытость и удобство работы пользователей.

В заключение отметим, что многозадачность прокурорской практики порождает необходимость увеличения интенсивности ее организационной составляющей, что обусловливает усиливающийся спрос на качественное применение информационно-коммуникационных технологий, которые необходимо рассматривать как значимый элемент управления.

Как видится, в дальнейшем вопросы применения информационно-коммуникационных технологий в органах прокуратуры в контексте организации работы и управления будут рассматриваться как существенно новые подходы в теории прокурорской деятельности.

А.В. Поливанов,
аспирант Тюменского
государственного университета

Криминологическое разграничение форм девиантного поведения треш-стрима и пранка

XXI век ознаменовал себя эпохой технологического прогресса, который лег в фундаментальную основу динамического развития социальных явлений. Главным сопутствующим фактором динамического развития социальных явлений является сеть «Интернет», благодаря которой люди обозначают и презентуют себя в медиапространстве.

Главной медиаплощадкой, в рамках которой люди презентуют свои видеоролики, является видеохостинг.

Видеохостинг – это веб-сервис, позволяющий загружать и просматривать видео в браузере. Сегодня одним из самых популярных видеохостингов является YouTube. Имеются и иные ви-

деохостинги, такие как Rutube, Instagram, VKontakte, «Одноклассники».

Благодаря видеоблогингу за последние два года в обществе появились новые формы социального поведения – пранк и треш-стрим.

Пранк (prank) в переводе с английского языка означает шалость, шутка, выходка, проказа. Лица, практикующие пранк в обществе, называются пранкерами.

Пранк представляет собой огромный комплекс социального поведения, обусловленный применением действий лица, причиняющих ущерб устоявшимся социальным нормам под видом розыгрыша или шутки.

Принято считать, что пранк – это телефонное хулиганство, телефонный розыгрыш, но на самом деле это не так. В течение последних двух лет пранк как социальное явление преобразовал себя и может проявиться во многих формах социального направления.

Пранк делится на две формы: который публикуется на видеохостингах и в социальных сетях и который не публикуется.

В первом случае действие лица направлено на зарабатывание денежных средств за счет просмотров опубликованного материала на видеохостинге в сети «Интернет». От количества просмотров данного материала зависит его заработок. Помимо заработка пранкеры стремятся получить хайп. Хайп (hype) с английского языка переводится как агрессивная реклама, целью которой является формирование предпочтений потребителя, в российской социальной среде означает привлечь к себе внимание, создать шумиху вокруг себя, получить популярность. Хайп помогает пранкерам повысить свой медийный рейтинг, который позволяет им участвовать в иных медийных проектах.

Во втором случае действие лица направлено на удовлетворение своих развлекательно-деструктивных потребностей без опубликования своих действий на видеохостинге в сети «Интернет». Причиной такого поведения является получение дополнительных эмоций, желание разнообразить свой досуг и т.д.

Своими действиями пранк наносит урон человеческим ценностям, а также социальной идеологии, которая культивируется в нашем обществе с целью развития духовно-нравственных начал.

Треш-стрим также является новым социальным явлением, которое появилось в начале 2020 г.

Треш-стрим в отличие от пранка не имеет дословного перевода и состоит из двух слов.

Треш (от английского – trash) переводится как уродовать, поливать грязью, гнобить, общаться как с непригодным.

Стрим (stream) переводится как транслировать.

Треш-стрим применительно к нашему обществу означает трансляцию сцен оскорблений, издевательств, избиений и иных действий, причиняющих моральный, душевный, а также физический вред.

Лицо, практикующее треш-стрим, именуется треш-стримером. Он преследует определенные цели: извлечение материальной выгоды или получение хайпа. Одним словом, все, что положительно скажется на имидже треш-стримера.

Пранк и треш-стрим как два социальных явления схожи друг с другом. В одном и том же социальном поведении люди пытаются получить материальную выгоду или хайп, однако они имеют ряд разграничений.

По условию реализации. Лицо, в отношении которого практикуется треш-стрим, является партнером треш-стримера. Партнер заранее осведомлен обо всех действиях, которые будут осуществляться в отношении него, посвящается во все планы со стороны треш-стримера. Взаимоотношения между треш-стримером и его партнером имеют согласованный характер, партнер понимает и осознает риски и последствия всех действий. Лицо, практикующее треш-стрим, в отличие от пранкера не ставит перед собой цель продемонстрировать эмоции своего партнера, за основу берутся сами действия, проводимые в отношении партнера, которые по своему содержанию являются аморальными. Сюжет треш-стрима навязывается самими зрителями, которые вносят пожертвования в виде денежных средств, тем самым дают треш-стримеру задание, которое он должен выполнить в отношении своего партнера.

Главным условием пранка является эффект неожиданности. Если жертва пранка заранее будет осведомлена о действиях и намерениях пранкера, то осуществить над ней пранк невозможно. Таким образом, пранк не образует себя как социальное явление, так как его жертва не даст той психологической реакции, которую пытается побудить пранкер своими действиями. Например, молодой человек упал в вагоне электропоезда, имитируя внезапный приступ. При этом его сообщники выкрикивали фразы о наличии у него коронавируса, провоцируя панику среди пассажиров, которые незамедлительно покинули вагон[1].

По способу проявления в обществе. Пранк и треш-стрим используют разные способы проявления в обществе.

Пранк проявляет себя в обществе путем видеосъемки на камеру, видеомонтажа ролика и дальнейшего его опубликования на платформе видеохостинга, случаи пранка в формате онлайн-трансляции не зафиксированы, так как пранк – это определенный сюжет, реализуемый по задумке пранкера, не каждый случай пранка является успешным, поэтому отснятый видеоматериал всегда подлежит видеомонтажу.

Треш-стрим проявляет себя с помощью прямой онлайн-трансляции, которую могут просматривать сразу несколько участников онлайн-стрима. Треш-стрим не подлежит видеомонтажу и проявляет себя как социальное явление в режиме реального времени в период онлайн-трансляции. Треш-стример получает денежные средства в виде пожертвований непосредственно до начала или в период онлайн-трансляции треш-стрима.

По мотиву. Лицо, практикующее пранк, в отличие от лица, практикующего треш-стрим, может осознавать, что в его действиях присутствует общественная опасность, однако в рамках мотива не желает нанести урон правоотношениям, находящимся под угрозой уголовного наказания. Основным мотивом пранкера выступают шутка, розыгрыш, которые направлены на создание ситуации, формально содержащей признаки какого-либо деяния, предусмотренного Уголовным кодексом Российской Федерации.

---

[1] Постановление Черемушкинского районного суда г. Москвы от 10.02.2020 об избрании меры пресечения в виде заключения под стражу в отношении Джаборова Каромата.

Лицо, практикующее треш-стрим, осознает, что совершает общественно опасное деяние, однако оправдывается тем, что его партнер не возражает против действий треш-стрима, что с позиции уголовного права не позволяет привлечь треш-стримера к уголовной ответственности, так как партнер треш-стримера де-факто не является потерпевшим.

По цели. Треш-стример практикует треш-стрим с целью получить финансовый достаток от количества просмотров и пожертвований зрителей онлайн-трансляции.

Цель пранкера не всегда связана с заработком, бывают случаи, когда пранкер не снимает пранк на видео и не публикует его на видеохостинге. Пранк в данном случае является способом удовлетворения своих развлекательно-деструктивных потребностей. Например, из хулиганских побуждений совершил звонок с заведомо ложным сообщением о готовящемся взрыве. В ходе судебного заседания он пояснил, что, заметив таксофон, доступный для бесплатного звонка, решил пошутить и, позвонив в любую службу, сообщить о каком-либо происшествии. Он придумал, что якобы видел, как неизвестный мужчина положил в мусорную корзину пакет с торчащими из него проводами, по внешним признакам похожий на взрывное устройство[1].

По родовому объекту. Рассматривая пранк с позиции уголовного права, можно сказать, что действия пранка являются родовым объектом преступлений против общественной безопасности и общественного порядка, так как создают реальную угрозу причинения вреда безопасным условиям жизни общества.

Родовым объектом треш-стрима являются преступления против личности, так как их действия наносят урон физической безопасности человека, которые сосредоточены в трех предметах: жизни, здоровье и внешних условиях, благоприятных для жизни и здоровья.

В заключение необходимо сказать, что наше общество столкнулось с двумя новыми формами девиантного поведения, которые на первый взгляд являются схожими. Однако, проведя

[1] Архив Александровского городского суда Владимирской области. Уголовное дело № 1-24/2020.

исследование, можно сделать вывод, что это два разных социальных явления, которые должны подлежать криминализации в виде отдельной статьи либо в виде составообразующего признака соответствующих статей Особенной части Уголовного кодекса Российской Федерации. Также необходимо выработать основные криминологические направления предупреждения и предотвращения пранка и треш-стрима в нашем обществе.

Секция 3.
Цифровые технологии в правоохранительной деятельности

Л.В. Голоскоков,
ведущий научный сотрудник
научно-исследовательского
отдела Московской академии
Следственного комитета
Российской Федерации,
доктор юридических наук,
доцент

Правоохранительные органы в замкнутом круге цифровых и других высоких технологий

Конференции на тему использования цифровых технологий для борьбы с преступностью важны и нужны, но не учитывают некоторые важные идеи.

Рассмотрим два круга, в которых происходит правоохранительная и научная деятельность.

Круг латентности. О порядке цифр латентности при легализации преступных доходов специалисты пишут: «Н.Н. Макарова отмечает, что раскрывается фактически лишь одно преступление из десяти. По мнению М.Е. Белая, примерный коэффициент латентности составляет 1:200. О высоком уровне латентности легализации преступных доходов в целом свидетельствуют результаты проведенного нами опроса, в ходе которого 83% респондентов указали, что уровень латентности данных преступлений превышает 75%, и лишь 17% определили его от 50% до 75%»[1]. Заметим, что легализация доходов осуществляется в том числе с помощью цифровых технологий, а здесь нас заинтересовал уровень оценки латентности 1:200, что можно изобразить в виде малень-

[1] *Зимин О.В., Быстрова Ю.В.* Некоторые аспекты криминологической характеристики легализации преступных доходов // Вестн. Акад. экон. безопасности МВД России. 2009. № 2. С. 70.

кого черного круга, расположенного в центре большого белого круга. Черный круг – область действия УК РФ, и его площадь показывает раскрытые преступления. Большой белый круг показывает поле нераскрытых преступлений, подпадающих под действие УК РФ (поле латентности).

Круг времени. Белое поле на краях большого круга расширяется, и это растущее во времени поле не урегулировано УК РФ. В нем совершается основное количество деяний, которые не являются преступными, но похожи на них, являются ими по сути дела, но не по форме (например, отток или вывоз капитала из страны). Возможно, УК РФ назовет их преступными через много лет, когда пройдет много научных конференций, правоведы и законодатель разберутся с терминами, сформулируют понятийный аппарат и т.п.

Преступность в сфере новых технологий всегда опережает правоохранительные органы. Новое и сложное трудно освоить, и этим пользуются преступники, имеющие более фундаментальное образование в сфере высоких технологий, чем сотрудники правоохранительных органов.

Суть замкнутого круга: раньше воровали коней, потом угоняли машины, сложнее оказалось ловить преступников, использующих машины и цифровые технологии. В описании этого «прогресса» постоянно возникает круг, в который попадают правоохранительные органы. Это не только круг, но и временно́й цикл, поскольку время течет не только однонаправленно, но и циклично, и новый цикл развития технологий возникает быстрее предыдущего, а технический уровень проблем растет по экспоненте.

Новые виды преступности мы обсуждаем на конференциях так же неспешно, как и полвека назад уличное хулиганство, которое тогда удалось одолеть. Но время ускоряется, и нужно думать не только о применении цифровых технологий в борьбе с преступностью, но и о том, как будут опережающим образом использовать их преступники и почему мы будем идти в хвосте цепочки событий: новая технология, применение ее преступником, запоздалое вступление в гонку правоохранителей, рост круга латентности, описанного нами, но с еще худшим соотношением раскрытых и нераскрытых преступлений.

В фильме полувековой давности «Берегись автомобиля» автоинспектор на старом мотоцикле говорит угонщику новенькой «Волги»: «И у меня привычка: ты удираешь, а я догоняю». Мы попали в этот же привычный круг – разве современный обобщенный правоохранитель имеет более серьезные средства, чтобы догнать ушедших в отрыв киберпреступников? Прошло полвека, но ситуация та же. Технологии в каждом цикле все новее, а ситуация старая.

На научных конференциях из года в год обсуждается вопрос противодействие преступлениям. Мы поставили себя в положение вечно догоняющего инспектора, которому не приходит в голову мысль о том, что *противо*действие есть явление вторичное, идущее в ответ на действие. Преступник действует, а органам не поставлена задача думать об опережающем преступность действии. Это причина появления порочного круга. «Вышел бы, помог завести мотоцикл», – просит автоинспектор угонщика в фильме. В жизни так и получается – нужно приглашать специалиста в помощь следствию, чтобы переиграть компьютерного преступника. И сегодня, как и угонщик Деточкин в фильме, специалист в сфере IT днем может быть экспертом, а ночью атаковать банковские счета своих жертв.

Что изменилось? Ничего: пеший хозяин лошади не мог догнать конокрада, угонщика новой машины – автоинспектор на старом мотоцикле, сегодня следователь в регионе не всегда имеет в кабинете Интернет. Но это уже вопросы не технологий, а концептуальные – хотим мы только противодействовать преступности или пойдем на опережающее действие. В свое оправдание мы можем сказать: никто не мог подумать, что технологии шагнут так далеко – киберпреступность! Но ведь и автоинспектор полвека назад не мог предположить, что будет догонять новую «Волгу» на мотоцикле-развалюхе. Как видим, оправдание не проходит: порочный замкнутый круг повторяется в своей сути, а не в технической составляющей.

Мы застряли в кругу старых проблем потому, что не решен вопрос концептуальный. Он не решается потому, что лежит в плоскости, в которой правоохранительные органы не работают в силу законов, регулирующих их деятельность. Заметим, что профилактика преступности – это другое. Это тактические и локальные мероприятия, а работа в рамках новой концептуальности –

деятельность стратегическая и глобальная, и она предельно широкая, затрагивающая вопросы общественного устройства. Сегодня этой деятельностью никто не занимается. Ничего в этом отношении не делать, никаких задач не ставить, но при этом хотеть развития, безопасности, отсутствия преступности и прочего – это наше удивительное текущее состояние.

Такой деятельностью могла бы заняться наука, но ведомственная наука зациклена на проблемах своей структуры, ее научная мысль в основном движется по спирали, направленной внутрь, в себя. В замкнутой системе нет решения всех ее проблем. Пример обхода этой опасности показали США: накопившиеся проблемы они сбрасывали во внешний мир путем экспансии доллара, навязывания стандартов, создания организаций типа ВТО, МВФ, путем войн, цветных революций и т.п. Это пример на политическом поле.

Наука тоже не должна замыкаться в себе. Это сегодня поняли в наших управленческих образовательных кругах после 30 лет деления наук на все более мелкие специальности. Начался процесс их укрупнения. Но кроме возвращения к междисциплинарным исследованиям нужна постановка глобальных целей, их нужно разработать, довести до общества, прийти к консенсусу.

Предположим, наука в поиске новой концептуальности получит результат. Наверняка он будет содержать неудобные выводы и предложения (лекарство всегда горькое). На каком-то высоком уровне идеи ученых могут не понравиться, исследования могут закрыть. Второй вариант: научные работы на эти темы вообще нигде не будут проводиться.

Разберем эту ситуацию с позиции направления экономической науки, которая называется «анализ рисков и экономическая безопасность». Эти отдельные лица (ученые, отделы, НИИ), выдвигая и реализуя идеи, берут на себя риски взаимодействия с начальством, обществом, государством. Эти риски разрешаются на уровне этих лиц за счет их благополучия, карьеры или жизни. Если запрещать исследования или не начинать их, не порождать новые идеи развития, произойдет накопление рисков, которые не смогут разрешиться на микроуровне, и тогда может произойти их переход на макроуровень, а это государство. Государство, не увидев их наличия, не разрешив их, может не справиться с лавиной рисков.

По закону, подобному закону сохранения энергии, риски не исчезают. Они могут накопиться, перейти с микроуровня на макроуровень и проявиться внутри другого объекта, в другой форме и с более серьезными последствиями. Когда это может произойти, неизвестно. Нет формул, методик, есть лишь приблизительное понимание, и его пока достаточно, чтобы приступить к работе.

Без решения этой задачи завтра мы не ответим на новые вызовы, как мы оказались не готовы решать проблемы криптовалют: Банк России известил в 2014 г. и в 2017 г., что криптовалюты «несут в себе высокие риски»[1]. Сомнения, опасения, промедление – 7 лет. Вместо действий.

Понимание важности управления рисками в сфере цифровой экономики показал Д.А. Медведев: «Уроки движения луддитов могут оказаться актуальными и для современного информационного общества»[2]. Луддиты – британские рабочие, которые в 1811–1817 гг. разбивали станки, несущие им безработицу. Сейчас ситуация может оказаться сложнее.

Нужно начать работу над новой концептуальностью (стратегии, концепции, доктрины) и понять, что должно представлять собой опережающее действие государства и правоохранительных органов, которое нужно будет делать, чтобы уйти только от противодействия. Противодействие как метод работы против преступности останется, но должно появиться и опережающее преступность действие. Концептуальность должна появиться на уровне государства, а правоохранительные органы будут применять свою часть общей концепции.

Почему ничего не создано в этом направлении? Никто не ставил такие задачи. В свое время не ставили задачу лететь в космос, ибо всем было очевидно, что это невозможно. Поставили задачу – полетели. Так и в науке – нужно поставить задачу. Пора размыкать замкнутый пока круг нашего противодействия преступности в сфере цифровых и других высоких технологий, иначе мы скоро попадем в следующий круг противодействия преступности, но уже в сфере каких-то еще более сложных технологий.

---

[1] Информация Банка России от 04.09.2017 «Об использовании частных «виртуальных валют» (криптовалют)» // Вестн. Банка России. 2017. № 80.

[2] *Медведев Д.А.* Россия-2024: Стратегия социально-экономического развития // Вопр. экономики. 2018. № 10. С. 11.

С.В. Зуев,
заведующий кафедрой
правоохранительной деятельности
и национальной безопасности
Южно-Уральского государственного
университета (НИУ), доктор
юридических наук, доцент

Цифровой правовой статус участника уголовного судопроизводства: понятие, признаки, содержание

В эпоху цифровизации уголовное судопроизводство, как и любое социальное явление, подлежит своего рода переформатированию. Всеобщее цифровое пространство бросает вызов всем сферам деятельности человека, в связи с чем появилась возможность и необходимость переоценить хорошо известные институты, нормы, правила процессуального поведения, а также используемый понятийным аппарат. Правовое положение участников уголовного судопроизводства испытывает обновление за счет внедрения новых информационных технологий в систему обеспечения их прав и реализации обязанностей. Правовой статус как мера возможностей в уголовном процессе приобретает цифровой оттенок. Пока это не рассматривается как первостепенное и неотъемлемое качество, но со временем оно может занять место очень значимого, если не основного, свойства.

Цифровой правовой статус участника уголовного судопроизводства – это совокупность информационно-телекоммуникационных возможностей, предусмотренных уголовно-процессуальным законом, использование которых зависит от включения физического или юридического лица в систему отношений уголовного судопроизводства посредством интернет-ресурсов или с помощью доступных электронных средств доказывания.

От процессуального статуса зависит доступность лиц, участвующих в уголовном деле, реализовывать свои права и исполнять обязанности, в том числе за счет цифровых технологий. Уже сегодня просматриваются определенные законом такие возможности.

Вместе с тем необходимо определять и вектор (перспективу) развития уголовно-процессуальных отношений в рамках цифрового правового статуса. Исходя из имеющихся процессуальных средств можно выделить некоторые признаки рассматриваемого явления и по ним ориентироваться на дальнейший генезис.

1. Представление электронных доказательств[1].

Традиционные материальные доказательства не теряют своего значения, однако все больше становятся востребованными цифровые. Согласно п. 4 ч. 2 ст. 42 УПК РФ потерпевший вправе представлять доказательства. Таким же правом обладают подозреваемый, обвиняемый, гражданский истец и гражданский ответчик, а также их представители. При этом положение ч. 2 ст. 84 УПК РФ определяет, что сведения в документах могут быть зафиксированы не только в письменном, но и в ином виде, а значит, и в электронном. Участник уголовного процесса может использовать любые доступные для восприятия с помощью технических средств материальные носители (флеш-накопители, смартфоны, видеорегистраторы и т.д.). Если электронные носители информации будут признаны вещественными доказательствами, то они приобщаются к уголовному делу в порядке ст. 81^1 УПК РФ. В перспективе ожидается, что электронные (цифровые) доказательства станут приоритетными, поскольку так называемое электронное уголовное дело предполагает полный переход на цифровую платформу осуществления уголовного судопроизводства.

2. Подача заявлений, ходатайств, жалоб в форме электронного документа.

Лицо, в отношении которого совершено преступление, вправе обратиться в правоохранительные органы с заявлением о преступлении через сайт государственных услуг, заполнив соответствующую интерактивную форму. Возможность подачи заявления в электронном виде закон прямо не предусматривает, но и не запрещает. Этот вопрос пока регламентируется подзаконными актами, что вряд ли можно считать достаточным. Так, приказом МВД России в Инструкции о порядке приема, регистрации и разрешения в территориальных органах Министерства внутренних дел Российской Федерации заявлений и сообщений о преступле-

[1] Подробнее см.: *Электронные* доказательства в уголовном судопроизводстве: учеб. пособие для вузов / отв. ред. С.В. Зуев. М., 2020.

ниях, об административных правонарушениях, о происшествиях, утвержденной приказом МВД России от 29.08.2014 № 736, закреплено: для приема заявлений о преступлениях, об административных правонарушениях, о происшествиях в электронной форме, направляемых посредством официальных сайтов, применяется программное обеспечение, предусматривающее обязательное заполнение заявителем реквизитов, необходимых для работы с заявлениями о преступлениях, об административных правонарушениях, о происшествиях. Электронные заявления распечатываются на бумажном носителе, дальнейшая работа ведется с ними как с письменными заявлениями о преступлениях, об административных правонарушениях, о происшествиях в порядке, предусмотренном данной Инструкцией.

К заявлению могут прилагаться какие-либо документы и материалы в электронном виде. Все это не исключает в дальнейшем предупреждение заявителя об уголовной ответственности за заведомо ложный донос в соответствии со ст. 306 УК РФ.

Данный вопрос также требует развития. Заявление, поступившее в электронном виде, может дублировать ранее принятое электронное заявление, содержать некорректные фразы и выражения, отражать событие некриминального характера. Заявителю может потребоваться помощь (консультация) в режиме онлайн. Необходимо совершенствование механизма идентификации заявителя и т.д.

В настоящее время завершается согласование федеральной целевой программы «Создание и внедрение государственной автоматизированной системы правовой статистики» (ГАС ПС), которой предусматривается введение до 2022 г. единой федеральной базы о зарегистрированных преступлениях в России. ГАС ПС будет представлять собой независимую систему учета, позволяющую отслеживать любое дело с момента его возбуждения до судебного решения. Граждане смогут подавать заявления о преступлениях в электронном виде и получать их номера в онлайн-режиме. В правоохранительных органах (СК России, МВД России, МЧС России, ФСБ России, ФТС России, ФСИН России) для ведения общей базы создадут автоматизированные рабочие места[1].

[1] URL: http://www.vedomosti.ru/politics/articles/2017/01/27/675123-prestupleniya.

Кроме того, согласно ч. 1 ст. 474[1] УПК РФ ходатайство, заявление, жалоба, представление могут быть поданы в суд в форме электронного документа, подписанного лицом, направившим такой документ, электронной подписью в соответствии с законодательством Российской Федерации, посредством заполнения формы, размещенной на официальном сайте суда в информационно-телекоммуникационной сети «Интернет». Материалы, приложенные к ходатайству, заявлению, жалобе, представлению, также подаются в форме электронных документов. Электронные документы, изготовленные иными лицами, органами, организациями в свободной форме или форме, установленной для этих документов законодательством Российской Федерации, должны быть подписаны ими электронной подписью в соответствии с требованиями законодательства Российской Федерации.

3. Участие в выборе электронных средств доказывания.

При участии потерпевшего или иного участника уголовного судопроизводства следователи могут проводить изъятие электронных носителей информации и копирование электронной информации. Эти два познавательных приема в некоторых случаях конкурируют между собой. Статья 164[1] УПК РФ в некоторой степени решает этот вопрос в пользу последнего познавательного приема, но императивно только по отношению к преступлениям в сфере предпринимательской деятельности. В остальных случаях все остается на усмотрение следователя. Вместе с тем участники следственного действия вправе независимо от категории преступления обратиться с ходатайством о копировании электронной информации, аргументируя свою просьбу убедительными доводами.

4. Участие в процессуальных действиях посредством видеоконференцсвязи.

Сегодня такая форма в большей степени применима для судебного рассмотрения уголовного дела, но в перспективе ожидается ее распространение и на стадию расследования преступлений[1], а в идеале и на все досудебное производство. Проблемным остается вопрос об установлении личности участника *видеокон-*

---

[1] *Дмитриева А.А.* Теоретическая модель безопасного участия личности в уголовном судопроизводстве: дис. … д-ра юрид. наук. М., 2017. С. 19.

ференцсвязи. Если непосредственное участие предполагает предоставление документа, удостоверяющего личность, то в онлайн-режиме вместо физического можно говорить об информационном присутствии, о демонстрации и визуальном сопоставлении изображения лица с фото на документе. Предупреждение об уголовной ответственности, заверенное подписью, подменяется видеофиксацией порядка разъяснения положений ст. 307, 308 УК РФ, что также требует дальнейшего совершенствования. Возможно, привязка каждого физического лица к его единому аккаунту в сети «Интернет» в какой-то степени положительно повлияет на решение многих вопросов.

5. Получение процессуальных документов в электронном виде.

Судебное решение, за исключением решения, содержащего сведения, составляющие охраняемую федеральным законом тайну, затрагивающие безопасность государства, права и законные интересы несовершеннолетних, решения по делам о преступлениях против половой неприкосновенности и половой свободы личности, может быть изготовлено в форме электронного документа, который подписывается судьей усиленной квалифицированной электронной подписью. В случае, если судебное решение вынесено судом коллегиально, оно подписывается всеми судьями, участвовавшими в рассмотрении дела, усиленной квалифицированной электронной подписью (ч. 2 ст. 474[1] УПК РФ). При этом экземпляр судебного акта в форме электронного документа хранится в правовой статистике государственной автоматизированной системы «Правосудие»[1].

В перспективе возможно развитие доступа участника уголовного судопроизводства не только к отдельным документам в электронном виде, но и ко всему уголовному делу в цифровом формате.

6. Использование искусственного интеллекта в работе с электронной информацией.

---

[1] Подпункт 2.1.9 приказа Судебного департамента при Верховном Суде РФ от 29.04.2003 № 36 «Об утверждении Инструкции по судебному делопроизводству в районном суде».

Сегодня в некоторых странах (в том числе в Китае[1], США[2]) активно внедряются, апробируются на практике программные системы с искусственным интеллектом по участию в рассмотрении уголовных дел.

Так, в Нью-Йорке алгоритмы, разработанные на основании обширной базы данных по завершенным делам, дают судьям рекомендации: отпустить под залог или заключить под стражу до суда человека, в отношении которого проводятся следственные действия.

Ученые строят прогнозы о появлении робота, который заменит следователя. Вместо следователя, сыщика в традиционном смысле субъектом расследования может быть программист, специалист по информационной безопасности (профессиональный антихакер), а также робот (компьютер)[3].

Представляется, что появление электронного помощника с заложенными возможностями искусственного интеллекта позволит оказать существенную помощь в раскрытии, расследовании преступлений и рассмотрении уголовных дел в суде.

Например, в Республике Азербайджан разработана программа «Электронные весы правосудия», призванная оказать помощь судьям в установлении размера наказания. В основе указанной электронной системы лежат матрица назначения наказания и алгоритмы его индивидуализации. В программу заложены рамочные правила, по которым определяются оптимальные меры наказания, учитываются обстоятельства, как смягчающие, так и отягчающие наказание. Все свойства метрически соизмеримы с положительными и отрицательными баллами. Используется общепризнанная формула «золотого сечения» и последовательность чисел Фибоначчи. Всего в систему заложено 25 алгоритмов, каждый из которых настроен на индивидуализацию наказания с учетом того, какое преступление совершено, а также данных о личности лица, его совершившего.

---

[1] URL: https://www.law.ru/article/22959-kradushchiysya-tigr-kak-iskusstvennyy-intellekt-stanovitsya-chastyu-sudebnoy-sistemy-kitaya

[2] URL: https://rg.ru/2020/04/26/iskusstvennyj-intellekt-nachal-evoliucionirovat.html

[3] *Власова С.В.* К вопросу о приспосабливании уголовно-процессуального механизма к цифровой реальности // Б-ка криминалиста: науч. журн. 2018. № 1. С. 16.

«Электронные весы правосудия» используются в тех случаях, когда судья считает невозможным прекращение уголовного дела. Система находится в совещательной комнате, куда уходит судья для вынесения приговора. Программа может работать в автоматическом и ручном режимах. Системная обработка данных позволяет выдать конкретные рекомендации по назначению оптимального размера наказания. Программа прошла апробацию и доказала, что позволяет минимизировать чрезмерно суровые наказания и избегать судебных ошибок[1].

Электронный помощник следователя может быть использован для ведения учета значимой для следователя информации (правовой, материалов проверок, шаблонов процессуальных документов, методических рекомендаций).

Важное место в расследовании преступлений занимает реконструкция криминального события. Цифровой ассистент следователя, используя математические методы, моделирование и автоматическую проверку информации, мог бы оказать существенную помощь в этом[2].

Таким образом, цифровой правовой статус сегодня – это гарантированный «талон» на участие в уголовном судопроизводстве; развивающееся уголовно-процессуальное явление; качество, присущее лицу, чьи права и законные интересы затрагиваются в процессе расследования или рассмотрения уголовного дела; еще одна «дорожка» в цифровой мир электронного правосудия.

---

[1] URL: https://az.sputniknews.ru/science/20181024/417556771/azerbaijan-uchenij-otkritie-pravosudie.html

[2] *Soltani S., Seno S.A.H.* A formal model for event reconstruction in digital forensic investigation Digital Investigation // Digital Investigation. 2019. 30. P. 148. URL: https://doi.org/10.1016/j.diin.2019.07.006

Л.И. Беляева,
профессор кафедры уголовной политики Академии управления МВД России, доктор юридических наук, профессор

Актуальные вопросы подготовки специалистов по информационной безопасности в высших учебных заведениях правоохранительных органов

Сегодня и в литературе, и в общении используется широкий спектр понятий и определений, относящихся к термину «безопасность». Это связано с тем, что основной документ, касающийся безопасности, содержит указание на то, что угрозы ей многообразны. Они могут носить социальный, политический, экологический, информационный, психологический, криминальный, военный и другой характер.

В их числе угрозы размывания традиционных российских духовно-нравственных ценностей и ослабления единства многонационального народа Российской Федерации путем внешней культурной и информационной экспансии (включая распространение низкокачественной продукции массовой культуры), пропаганды вседозволенности и насилия, расовой, национальной и религиозной нетерпимости, противоправных посягательств на объекты культуры[1].

Для предотвращения угроз национальной безопасности предусмотрены соответствующая правовая база, силы и средства, усилия уполномоченных на то органов, что составляет содержание уголовной политики, являющейся частью государственной политики в сфере обеспечения национальной безопасности. Круг возникших опасностей привел и к дифференциации мер, необходимых для неотложного реагирования. Так появились понятия «военная безопасность», «информационная безопасность», «личная безопасность», «противопожарная безопасность», «продовольственная безопасность», «финансовая безопасность», «эколо-

[1] Стратегия национальной безопасности Российской Федерации, утв. Указом Президента РФ от 31.12.2015 № 683.

гическая безопасность», «ядерная безопасность» и др. В этих понятиях находит отражение реальность имеющихся опасностей и их особенностей, являющихся основой для принятия соответствующих решений. При этом в одних случаях вид безопасности связывается с тем, от какой опасности требуется защита. Например, экологическая безопасность. В других же вид безопасности предопределяется объектом защиты: общественная безопасность, экономическая безопасность и др. Однако некоторые понятия безопасности многомерны и охватывают собой и то, и другое. Так, под информационной безопасностью понимается защита информации от посягательств на нее в целях неправомерного использования и защита прав и законных интересов личности, общества и государства в информационном пространстве. А Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» прямо говорит об определенном объекте защиты детей от вредного влияния на них информации.

В числе субъектов, обеспечивающих информационную безопасность и защиту соответствующих объектов от вредного влияния информации, важную роль играют правоохранительные органы. В области информационной безопасности они имеют свои назначением осуществление деятельности по двум стратегическим направлениям:

1. Обеспечение безопасности применительно к использованию информации – безопасное использование различной информации внутри системы правоохранительных органов и внутри органов, входящих в нее; предупреждение противоправных посягательств на неправомерное использование этой информации, а также информации, находящейся в обороте в других структурах; выявление, пресечение, раскрытие и расследование фактов неправомерного использования информации.

2. Обеспечение защиты личности, общества и государства от вредоносного влияния информации.

Деятельность правоохранительных органов в этих направлениях имеет специфику и особенности, что указывает на необходимость соответствующей подготовки будущих специалистов к решению задач по обеспечению информационной безопасности в профессиональной деятельности. В целом можно определить

несколько категорий специалистов, необходимых для решения задач, стоящих перед правоохранительными органами: специалисты в области информационной безопасности и защиты информации (аналитики в области компьютерной безопасности, разработчики систем безопасности и средств ее обеспечения, инженеры, непосредственно осуществляющие безопасность и защиту); специалисты, обеспечивающие создание и эксплуатацию информационных систем, их администрирование и безопасность; специалисты в области прогнозирования криминального поведения, связанного с использованием информационного пространства; специалисты в области выявления, пресечения и расследования криминальных проявлений в информационном пространстве; специалисты в области использования ИИ; ИТ-специалисты; специалисты иных профилей, имеющие доступ к информационным системам и использующие их в профессиональной деятельности.

Очевидно, что подготовка специалистов в области информационной безопасности носит специализированный характер, обусловленный не только техническими средствами, но и спецификой деятельности правоохранительных органов в целом и особенностями деятельности конкретного правоохранительного органа и его структурных частей.

Из этого следует, что педагогические цели подготовки специалистов в образовательных организациях правоохранительных органов для обеспечения информационной безопасности состоят в том, чтобы сформировать понимание сущности и содержания государственной политики в области информационной безопасности; личную и профессиональную готовность к реализации в соответствии с профессиональным назначением государственной политики в области информационной безопасности; понимание важности проблем безопасности и значения своей деятельности для ее обеспечения; совокупность знаний о субъектах и объектах, угрозах и опасностях в области информационной безопасности; систему знаний о методах и средствах обеспечения информационной безопасности, в том числе в профессиональной деятельности; умения применять полученные знания в профессиональной деятельности и профессионально значимые в профессиональной деятельности навыки.

При этом важным является формирование культуры поведения в информационном пространстве, которая складывается из основ общей, правовой и профессиональной культуры. То есть специалисту должны быть свойственны личное понимание гуманистической ценности информационной деятельности в целом; культура личного общения и сотрудничества в информационном пространстве; нравственное поведение, как личное, так и профессиональное, в области информационных отношений; знание и выполнение правовых предписаний в области регулирования информационных отношений; прочная профессиональная подготовка в области информационных технологий; хорошо развитые умения и навыки использования информационно-технологических возможностей для решения профессиональных задач; развитое чувство личной ответственности за действия с использованием информационных ресурсов; знания и умения обеспечивать защиту информации и защиту от нее.

Безусловно, в каждой из указанных групп возможна своя классификация по профилю деятельности, по ее направлениям, по месту и роли в этой деятельности. Общим же здесь является обширная правовая база, на которой строится профессиональная деятельность.

Из сказанного следует, что специалист в области обеспечения информационной безопасности, работающий в правоохранительных органах, должен знать актуальность, значение, содержание и особенности обеспечения информационной безопасности в области использования компьютерных систем и технологий; систему и виды субъектов, обеспечивающих информационную безопасность; место и роль в обеспечении информационной безопасности конкретных субъектов; характеристики информационных систем как объекта защиты; систему правового обеспечения информационной безопасности и защиты информации в компьютерных системах; принципы и виды обеспечения информационной безопасности компьютерных систем (организационное, аппаратно-программное, ресурсное, кадровое); основы компьютерной вирусологии, методы и средства защиты от вирусов; правила и требования, предъявляемые к пользователям компьютерных систем и обеспечению информационной безопасности в информационных системах; характеристики личности, общества и госу-

дарства как объектов обеспечения информационной безопасности; виды и характеристика угроз информационного характера безопасности личности, общества и государства; система и виды субъектов, обеспечивающих информационную безопасность личности, общества и государства; правовое обеспечение защиты безопасности личности, общества и государства от вредоносной информации; организационное обеспечение информационной безопасности личности, общества и государства; обеспечение защиты информации и сведений, составляющих государственную, служебную и коммерческую тайну.

В контексте задач, стоящих перед правоохранительными органами, по обеспечению информационной безопасности специалист в этой области должен уметь выявлять, анализировать и оценивать характер угроз информационной безопасности в действующей компьютерной системе; принимать обоснованные решения по устранению выявленных угроз; осуществлять правоприменительную деятельность, связанную с предупреждением, выявлением, раскрытием и расследованием правонарушений; обоснованно использовать в пределах полномочий методы и средства обеспечения информационной безопасности компьютерных систем и сетей; своевременно использовать имеющиеся в распоряжении средства и методы обеспечения информационной безопасности личности, общества и государства; лично использовать методы и средства обеспечения информационной безопасности в действующей компьютерной системе.

Специалисту в области обеспечения информационной безопасности необходимы хорошо развитые навыки, связанные с защитой электронных документов и их отдельных элементов от изменений, независимо от характера, на основе использования базовых возможностей операционных систем; защитой электронных документов путем использования цифровых подписей и сертификатов; архивированием и резервированием документов; выявлением, обезвреживанием и удалением компьютерных вирусов; обновлением антивирусных программ.

Несмотря на то что деятельность специалистов правоохранительных органов по обеспечению информационной безопасности во многом основана на навыках эксплуатации технических средств, знаниях в области естественно-научных дисциплин, ее

суть составляет все-таки социальное содержание, поскольку все вопросы, возникающие в области информационных отношений, связаны с человеком. А поэтому характер таких отношений зависит от личности участника таких отношений.

Очевидно, что подготовка в высших учебных заведениях правоохранительных органов специалистов по информационной безопасности должна строиться на строгой системе междисциплинарных (межпредметных) связей, что позволяет сформировать профессионально значимые качества личности.

О.В. Расторопова,
старший научный сотрудник
НИИ Университета прокуратуры
Российской Федерации,
кандидат юридических наук

Применение интерактивных экспертных систем для выявления преступлений в сфере экономики (на примере кредитных преступлений)

Для современной финансово-экономической преступности характерно широкое применение компьютерной техники и информационных технологий. Основные усилия «высокотехнологичного» криминала сфокусированы на банковской сфере, причем многие из технических приемов оказываются неожиданными для служб информационной безопасности коммерческих банков.

Ряд новых проблем в кредитно-финансовой сфере связан со все более широким применением электронных документов и различных видов электронной подписи. Многие ученые и специалисты-практики на основании проведенных исследований сделали выводы и о наличии ряда пробелов и противоречий в нормативных правовых актах, регламентирующих применение современной документированной информации в системе цифровых прав[1].

[1] *Волынский А.Ф., Прорвич В.А.* Электронное судопроизводство по преступлениям в сфере экономики (научно-практические аспекты): монография. М.: Экономика, 2019.

В связи с этим выявление признаков преступлений рассматриваемого вида, их раскрытие и расследование становятся особенно сложными, что требует разработки новых информационных технологий и инструментария. Одним из примеров научно обоснованных подходов при решении обозначенных проблем является недавно вышедшая монография, в которой описываются новые технологии для надлежащего расследования уголовных дел о преступлениях в сфере кредитования[1].

Здесь необходимо обратить внимание на то, что к таким преступлениям обычно относят мошенничество в сфере кредитования (ст. 159^1 УК РФ), мошенничество с использованием электронных средств платежа (ст. 159^3 УК РФ), включенные законодателем в гл. 21, а также ряд преступлений гл. 22 УК РФ. Прежде всего, это незаконное получение кредита (ст. 176) и злостное уклонение от погашения кредиторской задолженности (ст. 177).

Выявлению признаков данных преступлений, их раскрытию и надлежащему расследованию уголовных дел посвящено большое количество публикаций. Одно из наиболее полных комплексных исследований проблем выявления, раскрытия и расследования преступлений данного вида представлено в книге, подготовленной коллективом авторов, представляющих различные организации[2].

Отдавая должное труду наших коллег, считаем необходимым обратить внимание на то, что данные уголовно-правовые нормы нацелены, прежде всего, на пресечение незаконной деятельности заемщиков, наносящей значительный ущерб коммерческим банкам. Вместе с тем по результатам анализа многочисленных публикаций о банкротстве нескольких сотен коммерческих банков можно сделать вывод о том, что криминал проник и в деятельность банков.

В ряде работ перечисленных и иных авторов уделяется внимание и разработке проблем выявления, раскрытия и расследования преступлений, связанных с незаконной банковской деятель-

---

[1] *Волынский А.Ф., Прорвич В.А.* Компьютерная криминалистика в системе уголовно-правовой защиты «традиционной» и цифровой экономики: монография. М.: Экономика, 2020.

[2] *Организация* и методика расследования отдельных видов экономических преступлений / под ред. А.И. Бастрыкина, А.Ф. Волынского, В.А. Прорвича. М.: Спутник+, 2016.

ностью (ст. 172 УК РФ), а также с фальсификацией финансовых документов учета и отчетности финансовой организации (ст. 172[1] УК РФ). Преступления данного вида совершаются, как правило, руководителями банков либо их владельцами.

Привлечь их к ответственности сложно, поскольку ведение, хранение и использование банковской документации находятся в их сфере компетенции. Нельзя не учитывать и их практически неограниченные финансовые возможности не только по привлечению для своей защиты высококвалифицированных адвокатов, но и по организации противодействия деятельности правоохранительных органов, связанной с выявлением признаков преступлений данного вида, а затем и расследованием уголовных дел.

Аспекты противодействия расследованию преступлений в сфере экономики также подробно рассматривались в публикациях различных авторов. Предлагались и способы пресечения данного противодействия. Наиболее полным является, на наш взгляд, исследование коллектива авторов, в котором проанализированы основные источники юридических ошибок, допускаемых при выявлении, раскрытии и расследовании таких преступлений, и важнейшие способы их профилактики[1].

Анализ данных публикаций позволяет сделать ряд выводов о том, что во многих случаях преступная деятельность руководителей высшего звена неразрывно связана с преступлениями различного вида, совершаемыми другими сотрудниками банка. Эти преступления предусмотрены рядом статей, включенных законодателем в гл. 23 УК РФ. Прежде всего, речь идет о злоупотреблении полномочиями (ст. 201), коммерческом подкупе (ст. 204) и посредничестве в коммерческом подкупе (ст. 204[1]). При этом считаем необходимым обратить внимание на то, что данные виды преступлений могут образовывать реальные совокупности с перечисленными. Вместе с тем анализу особенностей приведенных преступлений, предусмотренных гл. 23 УК РФ, применительно к преступлениям в банковской сфере не уделяется должного внимания.

---

[1] *Ошибки* при раскрытии и расследовании экономических преступлений / под ред. А.И. Бастрыкина, А.Ф. Волынского, В.А. Прорвича. М.: Спутник+, 2018.

В связи с этим важно обратить внимание не только на очевидные связи преступлений, предусмотренных ст. 172 и 172^1, и преступлений, предусмотренных ст. 201, 204 и 204^1 УК РФ. Понятно, что директору банка для фальсификации документов финансовой отчетности необходима помощь главного бухгалтера либо его заместителя, а в ряде случаев и иных сотрудников. Некоторые из них могут стать соучастниками данных преступлений либо посредниками в коммерческом подкупе.

Более детальные исследования показывают, что выявление признаков преступлений против интересов службы в коммерческих и иных организациях, связанных с преступной деятельностью в конкретном банке, представляет особо сложную задачу. Достаточно обратить внимание на то, что преступления, предусмотренные ст. 172^1 УК РФ, отнесены законодателем к преступлениям средней тяжести. Соответственно, уголовная ответственность за приготовление к данному преступлению не предусмотрена. Это открывает ряд возможностей для ответственных сотрудников конкретного банка по вовлечению определенного сотрудника к приготовлению к данному преступлению, не опасаясь уголовной ответственности за соответствующие деяния.

Но нельзя игнорировать и реальные факты, выявленные на основе изучения нескольких десятков уголовных дел, показывающие наличие криминальных связей между заемщиками, оформляющими необходимые документы для получения кредита с помощью определенного сотрудника банка, с данным сотрудником, а нередко и с его непосредственным руководителем. То есть речь идет о реальной совокупности одного или даже нескольких преступлений заемщиков, предусмотренных ст. 159^1, 159^3, 176 и 177 УК РФ, и преступлений сотрудников банка, предусмотренных ст. 201, 204 и 204^1 УК РФ.

Установить наличие признаков совокупностей данных преступлений особенно сложно, тем более если вся документация была подготовлена в электронном виде. Для этого необходимо использование специальных информационных технологий с элементами искусственного интеллекта, позволяющих осуществлять надлежащую обработку информации, имеющей правовой статус. Многие из таких технологий описаны в указанных монографиях.

Кроме этого, выявление преступлений рассматриваемого вида и их совокупностей существенно осложняется наличием большого количества нормативных правовых актов, регламентирующих деятельность как самих коммерческих банков, так и их сотрудников. Речь идет не только о ряде положений Гражданского кодекса Российской Федерации, федеральных законов о Центральном банке Российской Федерации, о банках и банковской деятельности в Российской Федерации и др., но и о многочисленных подзаконных актах Центрального банка Российской Федерации.

Выявить определенную совокупность данных положений применительно к анализу законности определенных действий конкретных сотрудников конкретного коммерческого банка следователям сложно. Аналогичный вывод можно сделать и в отношении прокуроров, осуществляющих надзор за следствием. Из-за высокой трудоемкости такой деятельности нередко возникают упоминавшиеся юридические ошибки, из-за которых нарушается один из важнейших принципов уголовного судопроизводства – неотвратимости наказания преступников за совершенное деяние.

Проведенный анализ сложившейся ситуации показывает, что обрабатывать вручную столь обширные массивы информации, имеющей правовой статус, и следователям, и прокурорам сложно, если вообще возможно. В связи с этим возникает объективная необходимость разработки проблемно-ориентированных информационных технологий больших объемов информации, имеющей правовой статус. При этом нередко приходится констатировать, что в составе таких информационных технологий должны использоваться элементы искусственного интеллекта.

Многие из данных проблем, возникающих в современных условиях в реальной прокурорской практике, уже обсуждались нами[1]. Применительно к задачам, которые обсуждаются в настоящей работе, необходимо обратить внимание на то, что применение искусственного интеллекта для обработки больших инфор-

[1] *Расторопова О.В.* Эвристические подходы при использовании искусственного интеллекта в информационном обеспечении деятельности органов прокуратуры // Евраз. юрид. журн. 2020. № 10.

мационных массивов связано с использованием специальных компьютерных программ, работающих без участия человека[1].

Понятно, что ни следователь, выявляющий признаки приведенных совокупностей преступлений, ни прокурор, надзирающий за следствием, не имеют права делегировать свои полномочия, предусмотренные действующим законодательством, компьютерной программе, даже если ее назвали искусственным интеллектом. Такие программы могут использоваться лишь для того, чтобы предложить определенные варианты тех результатов, которые получаются при обработке информации с помощью компьютерной программы, причем с подробным разъяснением, на основе каких исходных данных и с помощью каких критериев были получены эти результаты.

Поэтому необходимые элементы искусственного интеллекта для обработки информации, имеющей значение для выявления признаков указанных преступлений и их совокупностей, могут быть использованы только в режиме развернутого диалога со следователем или прокурором. Подобные диалоговые компьютерные системы принято называть интерактивными экспертными системами[2].

Здесь следует подчеркнуть, что соответствующие компьютерные программы в рамках интерактивной экспертной системы позволяют не только организовать диалог следователя или прокурора со своим компьютером, оснащенным необходимым программным обеспечением. Эта экспертная система по своим функциям может играть роль справочной системы, подобной широко используемым КонсультантПлюс, Гарант и т.п., а также стать помощником следователя, выполняющим его конкретные задания, связанные с выявлением, раскрытием и расследованием конкретных высокотехнологичных преступлений в сфере кредитования.

Что касается практической реализации такого рода интерактивных экспертных систем, то в литературе описаны примеры создания подобных информационных технологий и программного

---

[1] *Волынский А.Ф., Прорвич В.А.* Электронное судопроизводство по преступлениям в сфере экономики (научно-практические аспекты): монография.

[2] *Волынский А.Ф., Прорвич В.А.* Компьютерная криминалистика в системе уголовно-правовой защиты «традиционной» и цифровой экономики: монография.

обеспечения. Вместе с тем проведенный анализ показывает, что в их основу заложены такие алгоритмы обработки информации, которые существенно отличаются от алгоритмов, используемых для выявления, раскрытия и расследования преступлений в сфере кредитования. Но внести в них необходимые дополнения и корректировки возможно. Для этого необходимо выполнение совместных исследований и разработок представителей прокуратуры и специалистов по информатике и программированию.

К.Н. Евдокимов,
доцент кафедры государственно-правовых дисциплин Иркутского юридического института (филиала) Университета прокуратуры Российской Федерации,
кандидат юридических наук, доцент

Противодействие компьютерной преступности в Российской Федерации: понятие, система, состояние, тенденции

Компьютерная преступность в настоящее время является одной из основных угроз национальной безопасности Российской Федерации и причиняет российской экономике огромный вред.

Так, по экспертным оценкам, ущерб экономике России в 2018 г. от компьютерных преступлений составил более 1,1 трлн руб.[1], в 2019 г. – около 2,5 трлн руб., предполагаемый экономический ущерб Российской Федерации от компьютерной преступности в 2020 г. оценивается в 3,5–3,6 трлн руб.[2]

Анализируя состояние и динамику компьютерных преступлений, можно констатировать значительное увеличение количества деяний, совершенных с использованием информационно-

[1] *Сбербанк* прогнозирует ущерб экономике России от киберугроз в 2018 году в 1,1 трлн рублей. URL: https://www.kommersant.ru/doc/3676752 (дата обращения: 07.02.2021).
[2] *Сбербанк* оценил ущерб экономике России от кибератак в 2019 году в 2,5 трлн рублей. URL: https://www.kommersant.ru/doc/4226302 (дата обращения: 07.02.2021).

коммуникационных технологий (в 2018 г. – 174 674 преступления, в 2019 г. – 294 409, в 2020 г. – 510 396)[1].

Поэтому для нейтрализации данного антисоциального явления обществом и государством сформирована система противодействия компьютерной преступности.

Под противодействием компьютерной преступности автор понимает деятельность уполномоченных в соответствии с законодательством субъектов права по применению общих и специальных мер для предупреждения компьютерной преступности, в том числе по выявлению и последующему устранению факторов, способствующих совершению компьютерных преступлений (профилактика компьютерной преступности); выявлению, пресечению, раскрытию и расследованию компьютерных преступлений (борьба с компьютерной преступностью); минимизации и (или) ликвидации последствий проявлений компьютерной преступности (нейтрализация последствий компьютерной преступности).

При этом с организационной точки зрения система противодействия компьютерной преступности включает в себя такие элементы, как объекты криминологического воздействия, субъекты противодействия преступности, цель, задачи, принципы, меры противодействия преступности.

В качестве цели системы противодействия компьютерной преступности выступает защита конституционного строя Российской Федерации, ее суверенитета и территориальной целостности, прав и законных интересов личности, общества, государства от компьютерных преступлений, в том числе от преступных посягательств организованных преступных групп, специальных и разведывательных служб иностранных государств, террористических и экстремистских организаций, использующих в своей противоправной деятельности информационные, коммуникационные, компьютерные и иные высокие технологии.

К числу основных задач системы противодействия компьютерной преступности можно отнести, например: осуществление государственной политики и нормативно-правового регулирования в сфере противодействия компьютерной преступности; пре-

[1] URL: http://www.genproc.gov.ru (дата обращения: 07.02.2021).

дупреждение совершения компьютерных преступлений как лицами, привлеченными к уголовной ответственности за подобные деяния, так и иными лицами; выявление и своевременное устранение факторов, влияющих на совершение компьютерных преступлений; выявление, пресечение и раскрытие компьютерных преступлений органами дознания, а также иными уполномоченными в рамках своей компетенции органами государственной власти и местного самоуправления, гражданами и их объединениями.

Система противодействия компьютерной преступности функционирует на принципах законности, соблюдения прав и свобод человека и гражданина, свободы экономической деятельности, гласности, неотвратимости наказания за совершенное преступление; использования в деятельности современных достижений науки и техники, технологий и информационных систем; сотрудничества и координации деятельности правоохранительных органов, взаимодействия органов власти с институтами гражданского общества, международного сотрудничества и др.

Перечень объектов системы противодействия компьютерной преступности обширен, поэтому в качестве примера можно выделить деятельность организованных преступных групп, использующих информационно-коммуникационные и компьютерные технологии для совершения преступлений в кредитно-финансовой и научно-технической сферах, включая хищение конфиденциальной информации (персональные данные, сведения, составляющие коммерческую, банковскую, налоговую, служебную, следственную и иные виды тайны); противоправная деятельность террористических и экстремистских организаций, использующих информационно-коммуникационные и компьютерные технологии для совершения преступлений; преступные посягательства на безопасное функционирование объектов критической информационной инфраструктуры Российской Федерации и т.д.

Субъекты системы противодействия компьютерной преступности разделяются на субъекты общей и специальной компетенции.

К субъектам общей компетенции мы можем отнести органы власти и должностных лиц, коммерческие и некоммерческие организации, граждан и их объединения, для которых противодей-

ствие компьютерной преступности не является основным направлением деятельности, например: Президента Российской Федерации, Совет Федерации Федерального Собрания Российской Федерации, Государственную Думу Федерального Собрания Российской Федерации, Правительство Российской Федерации, Центральный банк Российской Федерации, Военно-промышленную комиссию Российской Федерации, органы власти субъектов Российской Федерации, органы местного самоуправления, средства массовой информации, граждан и их общественные объединения.

В круг специальных субъектов противодействия компьютерной преступности полагаем возможным включить: Совет Безопасности Российской Федерации, федеральные органы исполнительной власти (МВД России, ФСБ России, Роскомнадзор), органы судебной власти, органы прокуратуры Российской Федерации; следственные органы Следственного комитета Российской Федерации, специализированные коммерческие и некоммерческие организации.

Как уже указывалось, количество зарегистрированных правоохранительными органами компьютерных преступлений за последние три года увеличилось со 174 674 до 510 396, т.е. почти в три раза.

При этом в 2018 г. из 174 674 зарегистрированных преступных деяний данного вида в суд направлены уголовные дела о 36 767 преступлениях (21,05%), в 2019 г. – из 294 409 преступлений в суд направлены уголовные дела о 57 221 деянии (19,43%), в 2020 г. из 510 396 выявленных преступлений в суд направили уголовные дела с обвинительными заключениями о 82 977 деяниях (16,26%)[1].

Таким образом, рост на 292,2% с 2018 по 2020 г. количества выявленных (зарегистрированных) компьютерных преступлений показывает, что система профилактики компьютерной преступности практически не функционирует. Удельный вес деяний, уголовные дела о которых направлены в суд с обвинительным заключением, снизился с 21,05 до 16, 26%, что иллюстрирует низкую эффективность системы борьбы с компьютерными преступлениями.

[1] URL: http://www.genproc.gov.ru (дата обращения: 07.02.2021).

Следовательно, существующая система противодействия компьютерной преступности в настоящий момент неэффективна и требует серьезной модернизации как организационно-правовых основ, так и мер по профилактике, борьбе, нейтрализации проявлений компьютерных преступлений.

С учетом сказанного предлагаем следующие организационно-правовые меры по совершенствованию системы противодействия компьютерной преступности.

Для повышения эффективности системы противодействия компьютерной преступности следует расширить сферу деятельности негосударственных правоохранительных организаций: народных дружин (кибердружин), частных охранных предприятий, частных детективных агентств по выявлению, предупреждению, пресечению компьютерных преступлений путем обеспечения необходимым программно-аппаратным оборудованием и техническими специалистами, законодательного закрепления полномочий по охране компьютерной информации и информационно-коммуникационных сетей физических и юридических лиц, поиску утраченной компьютерной информации, выявлению и блокированию противоправного контента в информационно-коммуникационных сетях, включая сеть «Интернет».

С этой целью предлагаем:

дополнить Федеральный закон от 02.04.2014 № 44-ФЗ «Об участии граждан в охране общественного порядка» положениями о кибердружинах и кибердружинниках, уравняв последних по правовому статусу с народными дружинниками, предусмотрев государственную регистрацию кибердружин и включение их в региональные реестры общественных объединений правоохранительной направленности;

расширить содержание ст. 3 Закона Российской Федерации от 11.03.1992 № 2487-I «О частной детективной и охранной деятельности в Российской Федерации», включив в перечень видов охранных и сыскных услуг такие услуги, как охрана компьютерной информации, находящейся в собственности, во владении, в пользовании, хозяйственном ведении, оперативном управлении или доверительном управлении физических и (или) юридических лиц и поиск утраченной гражданами или предприятиями, учреждениями, организациями компьютерной информации.

Кроме того, автор приходит к выводу, что правовая основа противодействия компьютерной преступности состоит из большого количества нормативных правовых актов. В связи с этим требуется систематизация последних путем принятия кодифицированного федерального закона «О противодействии компьютерной преступности в Российской Федерации», который определил бы понятийно-терминологический аппарат, правовые основы противодействия компьютерной преступности, систему субъектов профилактики, борьбы и нейтрализации проявлений компьютерных преступлений, их полномочия и ответственность, общие и специальные меры противодействия компьютерной преступности.

Б.Ю. Житников,
профессор кафедры
информационных технологий
Владимирского филиала
Российской академии народного
хозяйства и государственной
службы при Президенте
Российской Федерации,
доктор технических наук,
профессор

Некоторые аспекты противодействия телефонному мошенничеству

Одним из прибыльных и относительно безопасных для правонарушителей способов совершения мошеннических действий является использование в качестве средства совершения правонарушения мобильного телефона.

Для определения путей противодействия телефонным мошенникам составим усредненный алгоритм подготовки и совершения ими данного правонарушения.

1. Получение средств совершения телефонного мошенничества (под телефонным мошенничеством будем понимать мошеннические действия, при которых в качестве средства совершения

правонарушения используется мобильный телефон) – мобильного телефона и SIM-карты[1], которые не должны по своим идентификационным кодам (IMEI, абонентский номер и т.п.) раскрыть личность мошенника и его сообщников.

2. Выбор схемы телефонного мошенничества, например, путем ознакомления с материалами данной конференции или с информацией специализированных сайтов, посвященных обсуждению данных схем[2].

3. Реализация выбранной схемы.

Результативность данного этапа зависит от умения телефонного мошенника применять психологию работы с предполагаемой жертвой, используя для общения мобильный телефон[3].

Выявим причины, по которым мошенникам удается обмануть жертву, на основании проведенного анкетирования жителей Владимирской области[4]:

1) страх за родственников (жизнь, здоровье (в том числе COVID-19), свобода) (~27%);

2) доверчивость (~ 22%);

3) желание легкой наживы (~ 12%);

4) боязнь огласки личной информации (~ 11%);

5) любопытство (~ 10%);

6) отсутствие навыков самозащиты (~ 3%);

7) предрассудки (~ 2%);

8) иные причины (~ 13%).

На основании анкетирования мошеннические схемы были классифицированы на следующие категории.

1. Ваш родственник убил (сбил, покалечил…) *человека.*

Принцип совершения мошенничества – требование дачи взятки сотруднику правоохранительных органов для освобождения задержанного родственника.

---

[1] URL: https://vk.com/sim1003 (дата обращения: 13.01.2021).

[2] URL: https://coollib.net/b/449293-aleks-dann-zhuliki-moshenniki-aferistyi-nastavlenie-prostofilyam-i-instruktsii-moshennikam-kniga-1 (дата обращения: 11.01.2021).

[3] *Льюис Д.* Эффективное общение по телефону. Секреты телефонного общения. URL: https://psyfactor.org/lib/tm3.htm (дата обращения: 11.01.2021).

[4] В ходе анкетирования (декабрь 2019 г. – декабрь 2020 г.) обработано 87 анкет. Со слов респондентов, они сталкивались с телефонными мошенниками ~ 87% или знают об этом со слов близких родственников или хороших знакомых. Около 25% респондентов попадали в подобные ситуации более двух раз.

2. Попытка склонить предполагаемую жертву к осуществлению звонка на платный абонентский номер[1].

Принцип совершения мошенничества – предполагаемой жертве поступает исходящий вызов, ответить на который не представляется возможным из-за непродолжительности звонка. Предполагаемая жертва перезванивает на номер, по которому с ней завязывают продолжительный разговор.

3. Пополнение счета телефона родственника, ошибшегося с переводом денег абонента и т.п.

Принцип совершения мошенничества – предполагаемой жертве поступает звонок телефонного мошенника, который:

представляясь родственником, просит срочно пополнить счет телефонного номера, с которого поступил звонок, заверяя, что все объяснит позже;

взволнованно сообщает, что случайно ошибся, пополняя баланс своего мобильного телефона (посылается поддельное SMS-сообщение о переводе средств), и просит вернуть денежные средства.

4. Проблемы с банковской картой.

Принцип совершения мошенничества – на мобильный телефон предполагаемой жертвы осуществляется звонок от «сотрудника» банка. Сообщаемая информация касается блокировки банковской карты. Чтобы этого не произошло, телефонный мошенник предлагает:

позвонить оператору банка (применяется вариант звонка на платный номер);

под правдоподобным предлогом сообщить необходимые для входа в «личный кабинет» интернет-версии банка персональные данные.

5.Фишинг.

Принцип совершения мошенничества – телефонным мошенником составляется SMS-сообщение, в которое интегрируется ссылка на сайт мошенника, имитирующий интернет-магазин. В случае приобретения товара на сайте мошенника покупатель теряет свои денежные средства.

---

[1] URL: https://businessman.ru/kak-sdelat-platnyiy-nomer-mobilnogo-telefona-kak-zarabotat-na-platnom-nomere.html (дата обращения: 04.01.2021).

6. Короткие команды[1].

Существуют специальные команды, представляющие собой набор строго определенной последовательности знаков, с помощью которых можно запрашивать информацию о картах клиента банка, совершать платежи, переводы с помощью мобильного телефона.

Принцип совершения мошенничества – телефонным мошенником осуществляется звонок предполагаемой жертве и доводится информация о том, что телефонный мошенник – сотрудник технического отдела оператора сотовой связи и в связи со сбоем работы оборудования для продолжения обслуживания абонента необходимо введение «сервисного кода». В случае согласия происходит списание денежных средств в пользу телефонного мошенника.

7. Вы выиграли….

Принцип совершения мошенничества – на мобильный телефон потенциальной жертвы поступает звонок (или приходит SMS-сообщение) от юридического лица с поздравлением о выигрыше. Для получения солидного выигрыша предлагается перевести небольшую сумму денег оргкомитету. В случае согласия деньги переходят к телефонному мошеннику.

8. Заплати за операцию.

Принцип совершения мошенничества – телефонный мошенник представляется врачом и сообщает, что родственник предполагаемой жертвы госпитализирован и нуждается в неотложной медицинской помощи, за которую необходимо заплатить определенную сумму. Решение нужно принять быстро, так как любое промедление может привести к летальному исходу.

9. *«Если вы не переведете деньги, то ваш близкий родственник умрет в течение недели».*

Сообщение адресовано людям, которые верят в черную магию, колдовство. Принцип совершения мошенничества – на телефон потенциальной жертвы приходит SMS-сообщение с указанным текстом.

10. *Avito.ru телефонное мошенничество.*

Принцип совершения мошенничества – продавцу поступает звонок от телефонного мошенника, который сообщает, что готов купить и оплатить товар. Далее:

---

[1] URL: https://www.sberbank.ru/ru/person /dist_services/ussd (дата обращения: 30.12.2020).

потенциальной жертве перезванивает телефонный мошенник и просит сообщить ему пароль из SMS-сообщения для осуществления перевода денег (т.е. компрометация информации для входа в мобильный банк);

или после согласия о сделке с использованием Avito-доставки на телефон потенциальной жертвы приходит фиктивное SMS-сообщение об оплате товара по системе Avito-доставка. Получив данное сообщение, потенциальная жертва отправляет товар телефонному мошеннику.

11. *COVID-19.*

Принцип совершения мошенничества – потенциальной жертве поступает телефонный звонок с предложением (например, запись на вакцинацию, продажа лекарств от коронавируса, услуги по обработке помещений и т.п.), но для подтверждения намерений об оказании предлагаемой услуги мошенник просит перевести определенную сумму денег на свой счет.

В качестве первостепенной меры противодействия телефонному мошенничеству предлагается создание условий, при которых правоохранительные органы могли бы быстро установить лиц, использующих средства мобильной связи для осуществления мошеннических действий:

1. Провести комплекс мероприятий, которые позволили бы в дальнейшем по телефонному номеру установить личность владельца.

2. Предусмотреть при заключении договора сотовыми операторами связи на оказание услуг сотовой связи обязательное включение в договор EMEI сотового аппарата. Для реализации данного предложения следует:

1) установить срок, в течение которого все владельцы SIM-карт должны посетить офисы операторов сотовой связи для подтверждения своей личности;

2) после установленного срока SIM-карты, владельцы которых не подтвердили свою личность, должны быть исключены из обслуживания сотовыми операторами связи;

3) приобретение (получение) SIM-карты должно проходить исключительно в офисе сотового оператора с обязательным фотографированием процесса оформления для возможности идентификации и аутентификации личности продавца и покупателя;

4) после выполнения подп. 1–3 дополнить ГК РФ статьей, предусматривающей, что в случае совершения мошеннических действий с использованием SIM-карты, которую обслуживает оператор сотовой связи с нарушением установленного порядка заключения договора на оказание услуг сотовой связи, возмещение ущерба при приостановлении предварительного следствия по п. 1 ч. 1 ст. 208 УПК РФ возлагается на оператора сотовой связи в полном объеме;

5) после выполнения подп. 1–3 дополнить ГК РФ статьей, предусматривающей, что в случае совершения мошеннических действий с использованием SIM-карты, добровольно переданной лицом, заключившим договор с оператором сотовой связи, третьему лицу, возмещение ущерба при приостановлении предварительного следствия по п. 1 ч. 1 ст. 208 УПК РФ возлагается на лицо, заключившее договор с оператором сотовой связи, в полном объеме;

6) предусмотреть в личном кабинете оператора сотовой связи необходимость в определенный срок (например, в течение 3 дней) лицом, использующим сотовый телефон, который уже использовался хотя бы один раз с другой SIM-картой, зарегистрировать данный аппарат (по EMEI) на себя.

Безусловно, предложенные меры не смогут полностью искоренить данного вида мошеннические действия, но будут эффективным средством противодействия расширению данного негативного явления. Заметим, что иные меры противодействия телефонным мошенникам не дали положительного результата[1] и не помогли предотвратить его резкий рост в период пандемии 2020 г.

[1] URL: https://tass.ru/ekonomika/10341633; URL: https://lenta.ru/news/2020/12/24/crime/; https://genproc.gov.ru/smi/news /regionalnews/news-1843718/ (дата обращения: 14.01.2021).

Е.А. Киселёв,
доцент кафедры криминалистики
Хабаровского филиала
Московской академии
Следственного комитета
Российской Федерации»,
кандидат юридических наук,
доцент

Особенности тактики проведения следственных действий при расследовании уголовных дел о преступлениях, совершаемых с использованием современных информационных и телекоммуникационных технологий

Развитие информационных и телекоммуникационных технологий обусловило рост количества преступлений в сфере компьютерной информации.

При расследовании уголовных дел о преступлениях, совершенных с использованием современных цифровых и телекоммуникационных технологий, особое внимание следует обращать на порядок получения и фиксации криминалистически значимой информации. Этот порядок обусловлен, прежде всего, спецификой и правовым регулированием обращения этой информации[1].

В ходе расследования уголовных дел о подобных преступлениях нередко изымаются электронные носители информации. Среди них выделяется цифровая техника, находящаяся у потерпевшего, подозреваемого, (обвиняемого). К проблемам осмотра этих объектов относится извлечение цифровой информации, хранящейся в памяти исследуемого устройства, и с его помощью с удаленных носителей. Фиксация цифровой информации, имеющей значение для расследования уголовного дела, при проведении следственного осмотра должна осуществляться не только в письменном виде в протоколе следственного действия, но и с использованием других способов и форм сохранения информации. К таковым можно отнести снимок экрана (скриншот) с последующей его распечаткой и приобщением к протоколу следственно-

[1] *Ким Е.П., Киселёв Е.А., Каравянская О.Н.* О криминалистической характеристике преступлений, совершаемых с использованием современных информационных и телекоммуникационных технологий // Науч. компонент. 2020. № 3 (7).

го действия, копирование структуры интернет-страницы при помощи специального программного обеспечения[1].

Следственный осмотр с участием специалиста отдельно стоящего компьютерного оборудования (рабочей станции, PC) предлагается проводить в следующей последовательности.

На первом этапе определяются расположение PC и периферийных устройств относительно друг друга на момент осмотра и в пространстве (локация); тип, марка, конфигурация, цвет, заводской и (если имеется) инвентарный номера системного блока и каждого периферийного устройства, входящего в его комплект; тип, цвет и индивидуальные особенности каждого соединительного и электроснабжающего провода, состояние PC на момент осмотра (подключение к электроснабжению); содержание информации на его мониторе; техническое состояние (внешнее состояние корпусов оборудования, комплектность, работоспособность устройств); тип источника электроснабжения, его тактико-технические характеристики и техническое состояние; подробно описываются изменения в компьютерном оборудовании, не предусмотренные стандартами конструкции.

На втором этапе в протоколе отражается осуществление сбора информации с участием специалиста в электронной форме: указываются аппаратно-программные средства, используемые специалистом, и порядок их подключения; наличие или отсутствие в осматриваемом компьютерном оборудовании программных средств защиты информации, ее считывания и отправки по техническим каналам; результаты тестирования с целью выявления скрытой, ранее уничтоженной информации; структура и содержание информации, хранимой в PC и периферийных устройствах. Затем производится упаковка в соответствии с законом в определенной последовательности носителей электронной информации и полученных бумажных носителей информации.

При работе с компьютером, подключенным к компьютерной сети, необходимо: отключить питание роутера или модема, отсоединить от разъема сетевой платы RJ-45 Ethernet-кабель, извлечь из USB-гнезда беспроводной USB WiFi-адаптер, тем самым обеспечив сохранность информации в PC от дистанционного удале-

---

[1] См.: *Использование* компьютерных технологий в деятельности следователя: монография / А.Ф. Родин, В.Б. Вехов; под ред. проф. Б.П. Смагоринского. Волгоград: ВА МВД России, 2003.

ния и изменения. Проводится встречная фотосъемка осматриваемых объектов и соединений в том положении, в котором они были обнаружены. Целесообразно также проведение ориентирующей и обзорной фотосъемки исследуемых объектов до изменения их первоначального положения.

Рекомендуется также фотосъемка текста, изображений, обнаруженных на экране включенного компьютера.

Если компьютер включен и экран пуст, целесообразно пошевелить манипулятор (мышь) или нажать «пробел». Это активизирует изображение на мониторе. После того как изображение появилось, сфотографировать экран.

При необходимости изъятия оборудования следует отсоединить электрокабель с тыльной панели корпуса системного блока, отметить и промаркировать кабели для последующей идентификации подключенных устройств; отключить все кабели и устройства от системного блока. Все изымаемые объекты упаковываются, хранятся таким образом, чтобы обеспечить их сохранность.

Перед изъятием информации необходимо проконсультироваться со специалистом, исключить доступ посторонних к указанным объектам, обеспечить бесперебойное питание сервера. Извлечение информации поручается специалисту.

При работе с устройствами для хранения информации необходимо по возможности изъять инструкции по эксплуатации, документацию и бумажные записи.

При составлении протокола сначала описываются внешние признаки носителя, а затем электронной информации. Фиксируются также признаки преступных действий, которые нередко отражаются в виде хранящейся, передаваемой с помощью осматриваемого носителя электронной информации.

Описание физических накопителей компьютерной информации (флеш-накопителей, оптических дисков, съемных винчестеров и т.п.) рекомендуется начинать с индивидуальных признаков защиты от подделки или несанкционированного копирования. Перед исследованием информации целесообразно ее копирование. Далее фиксируются общий объем носителя компьютерной информации, вид разметки, объем плоскости, свободной от записи информации, количество и номера сбойных зон, секторов, участков, количество записанных файлов, программ, каталогов и

логическая структура их размещения, формат и содержание каждого отдельного файла, программы. Необходимо техническим способом защитить физический накопитель от записи или стирания с него информации (упаковав соответствующим образом и предохранив от повреждений информацию)[1].

При работе с различного рода гаджетами (цифровыми фотокамерами, навигаторами, видеорегистраторами и т.п.) рекомендуется промаркировать и изъять все кабели (чтобы использовать в последующем в качестве зарядного устройства) вместе с устройством в заряженном состоянии. Если устройство не может поддерживаться в заряженном состоянии, его исследование должно быть проведено специалистом до того, как разрядится батарея автономного питания. Изымаются также дополнительные средства хранения информации (карты памяти memory stick, compact flash и т.д.).

Определенными особенностями отличается фиксация хода и результатов осмотра мобильного устройства (телефона). Сначала фиксируются место обнаружения этого объекта, его положение относительно других элементов обстановки. Затем описываются признаки передней, задней панели, информационного табло и всех слотов. В протоколе отражаются сведения о его функциях. Нужно иметь в виду, что в телефонах Android меню: «Настройки», «О телефоне», «Общая информация». В телефонах Ios меню: «Настройки», «Основные», «Об устройстве». Модель и IMEI телефона (GSM) указаны под аккумулятором сверху. IMEI можно определить набором комбинации *#06#. Способ получения информации необходимо отразить в протоколе осмотра. В нем также фиксируется наличие всех внешних источников (SIM-карты с указанием ICCID, карты памяти с указанием реквизитов), батареи, чехла. По возможности в протокол вносятся данные о журнале звонков. Для исключения дистанционного удаления данных мобильное устройство обязательно переводится в авиарежим[2].

---

[1] *Электронные* носители информации в криминалистике: монография / под ред. О.С. Кучина. М.: Юрлитинформ, 2017. С. 176.

[2] См.: *Технико-криминалистическое* сопровождение расследования преступлений: учеб. пособие / под. ред. А.М. Багмета. М.: Юрлитинформ, 2016.

При наличии пароля на доступ к телефону по возможности выяснить его у владельца телефона и внести в протокол[1].

При работе с любым компьютерным оборудованием в протоколе следственного действия рекомендуется отражать все действия с компьютерной техникой (нажатия на клавиши клавиатуры, порядок выключения и отсоединения проводов и т.д.) и их результаты (включая содержание прозвучавших в ответ звуковых фрагментов); место обнаружения каждого носителя компьютерной информации, характеристики обнаруженных, осмотренных и изъятых объектов (при описании системного блока персонального компьютера, модема, принтера и т.д. необходимо указать их размеры, название фирмы-производителя, марку, модель, серийный инвентарный номер). При описании отдельных носителей компьютерной информации – их идентификационные признаки, видимые невооруженным взглядом, – размеры, внешний вид, материал корпуса, тип (магнитный, оптический и т.п.), сведения о производителе, объем памяти, рукописные или заводские надписи на наклейках. По возможности описываются файлы (их атрибуты, даты, время создания и последней модификации), содержащие информационные следы преступных действий. При обнаружении внутри компьютерной техники нештатной аппаратуры она описывается с помощью специалистов.

В протоколе также фиксируется содержание обнаруженной в памяти устройства информации, имеющей значение для досудебного производства. Возможно также изготовление скриншотов этой информации, которая переносится на локальные носители, приобщаемые к материалам досудебного производства.

Для сохранения видеофайлов наиболее эффективно использование онлайн-сервисов, предназначенных для скачивания файлов. Например, сервис по адресу https://ru.savefrom.net позволяет сохранять на жестком диске компьютера видео, размещенное на различных веб-ресурсах и в социальных сетях. Для этого в адресной строке перед именем видеохостинга необходимо добавить символы ss. После переадресации появится меню с вариантами

[1] По вопросу соблюдения конституционного права на тайну переписки и неприкосновенности частной жизни при проведении осмотра мобильного устройства см.: определение Конституционного Суда РФ от 25.01.2018 № 189-О «Об отказе в принятии к рассмотрению жалобы гражданина Прозоровского Дмитрия Александровича на нарушение его конституционных прав статьями 176, 177 и 195 Уголовно-процессуального кодекса Российской Федерации».

сохранения видеофайла, будет предложено выбрать формат и качество сохраняемого видео.

При необходимости фиксации информации, находящейся на жестком диске компьютера, когда изъятие носителя невозможно, наиболее эффективным решением будет использование приема клонирования. Он заключается в создании копии жесткого диска путем переноса на другой носитель необходимых данных. В результате операции клонирования создается копия HDD- либо SSD-носителя на внешнем носителе с максимально идентичными исходному носителю параметрами информации. В этих целях могут быть использованы бесплатные программные продукты, имеющиеся в свободном доступе в сети «Интернет», например AOMEI Backupper, EaseUS Todo Backup, Macrium Reflect и им подобные, которые представляют собой средства для резервного копирования жестких дисков или их разделов, а также отдельных файлов. При проведении такой операции принимающий носитель должен быть по объему больше клонируемого.

К.В. Кузнецов,
помощник Московского
межрегионального транспортного
прокурора по организационным
вопросам, контролю исполнения,
кандидат юридических наук

Использование программно-технических средств обеспечения анонимности пользователей в информационно-телекоммуникационной сети «Интернет» как одно из средств совершения преступлений повышенной латентности

Наметившаяся тенденция роста количества так называемых киберпреступлений в широком смысле этого слова (в понимании, изложенном в так и не ратифицированной Российской Федерацией до настоящего времени Конвенции о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23 ноября 2001 г.), в соответствии с положениями которой компьютерные

системы, сети и компьютерные данные наряду с объектами преступных посягательств выступают в качестве орудий и средств их совершения) получила в минувшем году более отчетливые очертания.

В то же время ведущими криминологами высказывается обоснованная точка зрения о том, что развитие информационно-коммуникационных технологий, с одной стороны, способствует расширению сферы криминальных интересов и появлению новых преступных схем, усиливает организованность преступности, а с другой – фактически предоставляет возможность совершения киберпреступлений во многом безнаказанно и значительно увеличивает уровень их латентности[1].

В подтверждение сказанного обратимся к получившему широкое распространение на протяжении последних лет такому противоречивому явлению, как обеспечение анонимности пользователей в информационно-телекоммуникационной сети «Интернет».

Мониторинг данной сети свидетельствует о том, что наиболее популярным и эффективным способом обеспечения анонимности ее пользователей на данный момент является использование специализированных программно-технических средств. К их числу, в частности, относятся:

1) VPN или Virtual Private Network, что в переводе с английского означает виртуальная частная сеть. Использование технологии VPN позволяет обеспечить безопасный обмен информацией и файлами через общедоступную сеть «Интернет», поскольку указанная технология предполагает как использование шифрования данных, предотвращающих их перехват во время передачи, так и обеспечение анонимности самих пользователей сети, в том числе искажение сведений об их IP-адресе, местонахождении устройства (ПК или мобильного устройства), с которого осуществлен выход в сеть, и т.д.[2];

---

[1] *Комплексный* анализ состояния преступности в Российской Федерации и расчетные варианты ее развития: аналит. обзор / Ю.М. Антонян, Д.А. Бражников, М.В. Гончарова и др. М.: ФГКУ «ВНИИ МВД России», 2018. С. 64–65.

[2] *Николахин А.Ю.* Использование технологии VPN для обеспечения информационной безопасности // Экономика и качество систем связи. 2018. № 3. С. 61–62.

2) антидетект-браузеры (AntiDetect, AntBrowser, MultiLogin, Linken Sphere и др.), которые представляют собой видоизмененные пользовательские браузеры для работы в сети «Интернет», позволяющие пользователям вручную изменять настройки своей анонимности в сети (скрывать сведения о технических характеристиках устройств, с которых осуществляется выход в сеть, изменять IP-адрес и т.д.)[1];

3) использование технологии веб-прокси и прокси-серверов, позволяющих передавать в сети «Интернет» заведомо ложную информацию о пользователе и источнике направленного им запроса, а также обходить законодательно установленные запреты на осуществление доступа к тем или иным ресурсам в сети[2];

4) наконец, особый интерес представляет использование пользователями анонимных распределенных компьютерных сетей с «луковой» (сеть TOR) и «чесночной» (сеть I2P) маршрутизацией, которые благодаря применению особых технологий шифрования позволяют им обеспечить анонимность трафика и защиту передаваемых сведений и файлов, а также конфиденциальность информации о самих пользователях. Использование данных программно-технических средств позволяет пользователям получить непосредственный доступ к Darknet, который, по мнению многих специалистов, и является основной площадкой совершения преступлений в интернет-пространстве, фактически остающейся вне поля зрения правоохранительных органов[3].

Результаты изучения материалов судебной и правоприменительной практики позволяют констатировать, что преступные посягательства, совершаемые с использованием перечисленных программно-технических средств, являются наиболее трудновыявляемыми и обладают наивысшей степенью латентности.

---

[1] ТОП-10 антидетект-браузеров. URL: https://protraffic.com/articles/top-10-antidetekt-brauzerov-3231.html (дата обращения: 17.02.2021).

[2] *Галкин А.С., Архипов П.А., Маркин Д.О.* Организация анонимного доступа к удаленным ресурсам на основе технологии веб-прокси // Наукоемкие технологии в космических исследованиях Земли. 2016. № 8.

[3] *Джумадиль Е.Е., Макаревич М.Л.* Пути незаконного использования возможностей «Интернета» и вопросы правовой регламентации // Инновационная экономика: перспективы развития и совершенствования. 2018. № 2; *Узденов Р.М.* Новые границы киберпреступности // Всерос. криминолог. журн. 2016. Т. 10. № 4.

Фактически выявление и раскрытие преступлений, совершаемых с использованием информационно-коммуникационных технологий, осуществляется в нескольких случаях:

1) как правило, при проведении таких предусмотренных Федеральным законом от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности» оперативно-розыскных мероприятий, как оперативное внедрение и оперативный эксперимент;

2) если лица, осуществляющие преступную деятельность с использованием данных программно-технических средств, допустили какие-либо просчеты, позволившие получить их цифровые отпечатки, или совершили иные действия, благодаря которым осуществляющие оперативно-розыскную деятельность правоохранительные органы могут вычислить их вне цифровой среды;

3) если о готовящемся и (или) совершенном с использованием данных программно-технических средств преступлении (преступлениях) в уполномоченные правоохранительные органы сообщили лица, обладающие соответствующей информацией (как правило, соучастники преступлений).

При этом данные программно-технические средства обеспечения анонимности пользователей в сети «Интернет» открывают перед злоумышленниками практически неограниченные возможности для осуществления экстремистской и террористической деятельности, в том числе координации и финансирования деятельности соответствующих преступных формирований, осуществления торговли наркотическими средствами и психотропными веществами, а также их аналогами, оружием и боеприпасами, работорговли и торговли человеческими органами, совершения преступлений в сфере экономической деятельности, а также против собственности и т.д.

Таким образом, как справедливо отметил прокурор Московской области С.В. Забатурин, правоохранительная система пока не поспевает за вызовами в киберпространстве[1].

В числе причин сложившейся ситуации необходимо отметить следующие, являющиеся, на наш взгляд, наиболее значимыми:

несоответствие уровня профессиональной подготовки и квалификации сотрудников правоохранительных органов, осу-

---

[1] *Частников* узаконят. Прокуратура Московской области предложила принять новые правила для частных домов престарелых. URL: https://rg.ru/2021/01/18/reg-cfo/zabaturin-dlia-chastnyh-domov-prestarelyh-nuzhny-novye-pravila.html (дата обращения: 18.02.2021).

ществляющих оперативно-розыскную деятельность и расследование преступлений, совершаемых с использованием информационно-коммуникационных технологий, сложившейся криминогенной ситуации и уровню подготовки лиц, осуществляющих преступную деятельность в рассматриваемой сфере. Должное информационно-методическое обеспечение деятельности сотрудников силовых ведомств на данном направлении не организовано, необходимые специальные познания у них в подавляющем большинстве случаев также отсутствуют. В частности, ведомственными правовыми актами (наставлениями, инструкциями и т.д.), регламентирующими оперативно-розыскную деятельность органов внутренних дел, вопросы организации и проведения оперативно-розыскных мероприятий, тактики и методики проведения оперативно-розыскной деятельности в рассматриваемой сфере в целом должным образом не урегулированы. И это несмотря на то, что данными органами выявляется большая часть (свыше 90%) указанных преступлений;

до настоящего времени не получил окончательного решения вопрос о легальности использования перечисленных программно-технических средств обеспечения анонимности пользователей сети «Интернет» в Российской Федерации. Так, Федеральным законом от 29.07.2017 № 276-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» установлен запрет на обеспечение использования в Российской Федерации информационно-телекоммуникационных сетей, информационных систем и компьютерных программ для получения доступа к запрещенным информационным ресурсам. При этом соответствующие обязанности по обеспечению запрета доступа к данным ресурсам возложены фактически на владельцев таких сетей, систем и программ. Таким образом, названный законодательный акт лишь частично решил проблему недопустимости обеспечения свободного доступа к запрещенным ресурсам, включенным в соответствующий реестр Роскомнадзора[1]. В то же время фактическое использование данных анонимайзеров в иных противоправных целях

[1] Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено. URL: https://eais.rkn.gov.ru/ (дата обращения: 18.02.2021).

выявляется редко, что создает реальную угрозу национальной безопасности Российской Федерации.

В свете изложенного можно сделать неутешительный вывод о том, что организация работы в целом, материально-техническое и кадровое обеспечение деятельности российских правоохранительных органов в сфере пресечения, выявления и раскрытия преступлений, совершаемых с использованием информационно-коммуникационных технологий, не отвечают современным реалиям.

В качестве одного из путей решения данной проблемы некоторые авторы, в частности С.А. Губин, предлагают создание отдельной высокотехнологичной структуры, специализирующейся на системном техническом противодействии данным интернет-платформам[1]. О планах по созданию в обозримой перспективе в структуре МВД России киберполиции в декабре 2020 г. также сообщило руководство ведомства[2].

Разделяя данную точку зрения, отметим, что сегодня назрела острая необходимость принятия ряда организационных и законодательных мер, направленных на предупреждение, своевременное выявление и пресечение преступлений, совершаемых с использованием информационно-коммуникационных технологий.

К их числу наряду с созданием профильных подразделений силовых ведомств необходимо отнести более четкое определение правового статуса соответствующих программно-технических средств, их нахождения в гражданском обороте и условий использования конечными пользователями сети «Интернет» на территории Российской Федерации, построение эффективной системы контроля трафика, распространяемого с их помощью, а также совершенствование тактики осуществления оперативно-розыскной деятельности уполномоченными органами на данном направлении.

---

[1] *Губин С.А.* Организованная преступность: от воровских организаций до сообществ в сфере высоких технологий (заметки прокурора): монография. М.: ООО «Юрид. фирма «КОНТРАКТ», 2020. С. 111.

[2] *В структуре* МВД создается киберполиция. URL: https://rg.ru/2020/12/18/v-strukture-mvd-sozdaetsia-kiberpoliciia.html (дата обращения: 17.02.2021).

А.А. Лебедева,
доцент кафедры криминалистики
Московской академии
Следственного комитета
Российской Федерации,
кандидат юридических наук

Расследование киберпреступлений следователями СК России

В последние годы с учетом тотальной цифровизации всех сфер жизнедеятельности общества, особенно в условиях так называемой коронавирусной пандемии, возросло число киберпреступлений.

С учетом того, что большинство составов преступлений, прописанных в УК РФ, могут быть совершены в виртуальном пространстве или при помощи компьютерной техники, возникла острая необходимость в создании специализированного отдела по расследованию киберпреступлений и преступлений в сфере высоких технологий в Следственном комитете Российской Федерации.

В соответствии с нормами Федерального закона от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации» и ст. 51 УПК РФ следователи Следственного комитета Российской Федерации были правомочны расследовать киберпреступления и ранее, до создания специализированного подразделения в центральном аппарате ведомства.

Изначально на ведомство возложено расследование сложных и резонансных преступлений. В связи с рекордными темпами роста количества так называемых киберпреступлений, их направленностью на детскую, подростковую аудиторию, а также на конституционные свободы граждан, а в ряде случаев и на объекты стратегической инфраструктуры государства наделение Следственного комитета Российской Федерации новыми полномочиями объяснимо.

Так, по мнению А.И. Бастрыкина, новый отдел должен стать неким связующим элементом, сосредоточивающим и концентрирующим усилия различных государственных ведомств, научных

учреждений и специалистов для эффективного и слаженного противодействия преступным явлениям в информационной сфере[1].

Примеры деятельности подразделений СК России по противодействию и расследованию киберпреступлений, представленные в СМИ[2]

Март – апрель 2020 г.	ГСУ СК России по Санкт-Петербургу возбуждено уголовное дело по ч. 1 ст. 272 УК РФ (Неправомерный доступ к компьютерной информации). Следствием установлено, что к срыву уроков школьников причастен ведущий канала Russia Paver на платформе YouTube, который неоднократно (27.03.2020 и 06.04.20020) незаконно подключался к обучающему процессу в формате онлайн-трансляций, во время подключений представляясь сотрудником Министерства образования Российской Федерации, дискредитировал, вел себя вызывающе, хамил
В апреле 2020 г.	СУ СК России по Саратовской области возбуждено уголовное дело по факту публичной демонстрации порнографических материалов среди несовершеннолетних неустановленным лицом во время дистанционного обучения школьников
В мае 2020 г.	СК РФ возбуждено уголовное дело по факту так называемой кибератаки на официальный сайт «Бессмертный полк» с целью реабилитации фашизма. Поводом и основанием возбуждения уголовного дела стали факты размещения портретов нацистов на интернет-ресурсе в День Победы
26 июня 2020 г.	Сервис Центральной избирательной комиссии Российской Федерации подвергся DDoS-атаке, направленной на срыв досрочного электронного общероссийского голосования по внесению поправок в основной закон Российской Федерации
Январь 2021 г.	Следственный комитет Российской Федерации возбудил уголовные дела по факту вовлечения несовершеннолетних в участие в несанкционированных акциях протеста через социальные сети TikTok, «ВКонтакте», Facebook, Twitter, Instagram, сервис YouTube

[1] См.: Интервью А.И. Бастрыкина 10 июля 2020 г. URL// https://www.interfax.ru/russia/716874 (дата обращения: 25.01.2021).
[2] Официальный сайт СК РФ. URL// https://sledcom.ru/ (дата обращения: 25.01.2021).

Несовершеннолетние лица более уязвимы на просторах сети «Интернет», чем в обычной социальной действительности. Преступнику, пользующемуся преимуществами интернет-пространства (отсутствие физического контакта жертвы и преступника), легче войти в доверие к несовершеннолетнему, используя мнимый созданный профиль, обманом, хитростью и психологическими манипуляциями склонить к совершению определенных, нужных преступнику действий.

В настоящее время следователи подразделений Следственного комитета Российской Федерации качественно расследуют и направляют в суд уголовные дела о киберпреступлениях, затрагивающих права и интересы в том числе несовершеннолетних граждан.

Так, СУ СК России по Оренбургской области направлено в суд уголовное дело, возбужденное по факту оборота порнографических изображений малолетних, совершенного жителем Матвеевского района Оренбургской области, 1986 года рождения.

Следствием установлено, что обвиняемый в период 2018–2019 гг. в социальных сетях под вымышленным профилем знакомился и общался с лицами, не достигшими четырнадцатилетнего возраста. Под различными поводами обвиняемый инициировал отправку ему порнографических снимков протерпевшими, позже распространял фотографии в сети «Интернет».

В рамках расследования уголовного дела собрана доказательственная база по 18 эпизодам совершения обвиняемым незаконных действий в отношении восьми малолетних потерпевших, шестеро из которых проживают в различных субъектах Российской Федерации[1].

Несмотря на то что потерпевшие находились в различных регионах, СК России своевременно отреагировал на сообщение о преступлении, проверочные действия осуществлены незамедлительно, возбуждено уголовное дело, в разумные сроки произведены необходимые следственные действия, в отношении подозреваемого избрана мера пресечения в виде заключения под стражу.

[1] Официальный сайт СК России. URL: https://sledcom.ru/ (дата обращения: 25.01.2021).

При производстве обыска в жилище подозреваемого ключевым моментом стал поиск мобильного телефона, ПК, различных съемных цифровых носителей, компьютерной техники с целью обнаружения на них видеозаписей, фотографий порнографического содержания несовершеннолетних потерпевших, электронной переписки с иными пострадавшими несовершеннолетними лицами[1]. Данные материалы составляют фундамент доказательственной базы по уголовному делу, поэтому их поиск, описание и фиксация в протоколе следственного действия, упаковка должны быть произведены с учетом всех требований законодательства.

В обвинительном заключении должны найти отражение способ совершения преступления, т.е. систематическое (с указанием периода) пользование страницей в социальной сети, с которой непосредственно велась переписка с несовершеннолетним потерпевшим лицом, адрес фактического местонахождения устройства (смартфона, ПК), с которого осуществлялся ввод диалогов с инициированием демонстрации и пересылки порнографических фото, адрес фактического нахождения обвиняемого, IP-адрес ПК, на чье имя и по какому адресу заключен договор с интернет-провайдером.

После обыска у подозреваемого и изъятия у него электронных устройств производится их тщательный осмотр, а также осмотр и извлечение содержащихся на них данных и информационных массивов, фото- и видеоконтента.

Отдельно стоит упомянуть о криминалистическом комплексе UniversalForensicxtractionDevice (UFED), который используется следователями-криминалистами СК России для извлечения так называемых цифровых следов преступлений из мобильных устройств.

Современная преступность бросает вызов правоохранительной системе в форме реализации преступного умысла в киберпространстве, сотрудники СК России компетентны расследовать преступления с учетом последних тенденций.

---

[1] См.: *Антонов О.Ю.* Типичные следственные ситуации при расследовании сексуальных преступлений, совершаемых с использованием информационно-телекоммуникационных сетей: специфические особенности и пути разрешения // Рос. следователь. 2018. № 2.

Т.В. Раскина,
ведущий научный сотрудник
НИИ Университета прокуратуры
Российской Федерации,
кандидат юридических наук

Проблемы противодействия треш-стримам как пример необходимости изменения тактики обеспечения законности в сфере информационно-коммуникационных технологий

Состояние законности в сфере информационно-коммуникационных технологий характеризуется быстрым и масштабным появлением различных деструктивных процессов, которые по темпам своей эволюции значительно опережают развитие регулируемых правом общественных отношений. Эти процессы связаны с различными вариантами хищения чужого имущества (carding, fishing, pharming, skimming), посягательствами на жизнь, здоровье, достоинство личности (sexting, gruming, bullying), общественную и государственную безопасность (кибертерроризм, киберэкстремизм) и др.

Правовая неурегулированность общественных отношений в сфере информационно-коммуникационных технологий является одной из основных детерминант возникновения указанных криминальных и иных негативных процессов. Скорость развития современных технологий и масштабы их применения настолько большие, что связанная с их использованием деятельность остается длительное время вне правового поля. Опасность ситуации заключается в невозможности своевременного реального обеспечения прав и свобод человека и гражданина, интересов общества и государства и их защиты.

Примеров этому немало[1]. Общественный резонанс вызвали события, когда в прямом эфире в сети «Интернет» стали транслироваться аморальные и преступные действия (треш-стримы), в

[1] *Бычкова А.М., Раднаева Э.Л.* Доведение до самоубийства посредством использования интернет-технологий: социально-психологические, криминологические и уголовно-правовые аспекты // Всерос. криминолог. журн. 2018. Т. 12. № 1. С. 101–115 и др.

том числе повлекшие смерть человека. При этом анализ нормативно-правовой базы показал, что в стране отсутствуют адекватные механизмы противодействия треш-стримам, а также фундаментальные эмпирические исследования данного явления. Конечно, во многом это связано с относительной новизной треш-стримов. Вместе с тем изучение имеющейся в открытых источниках информации свидетельствует о том, что данное явление несет в себе повышенную общественную опасность и высокий риск угрозы причинения вреда общественным отношениям в сфере охраны жизни и здоровья личности, имущественных и иных прав и свобод человека, общественной безопасности. Сложившаяся ситуация даже обусловила принятие решения о рассмотрении вопросов борьбы с треш-стримами на заседании одной из комиссий Совета Федерации Федерального Собрания Российской Федерации[1].

Треш-стрим представляет собой трансляцию (от лат. translatio – передача) высказываний и (или) действий, имеющих аморальный, асоциальный и (или) противоправный характер. Она осуществляется посредством публичной передачи визуальной информации в прямом эфире с использованием информационно-телекоммуникационных сетей и предназначена для неопределенного круга лиц. Разновидностью современного треш-стрима является хардтреш-стрим, когда высказывания и (или) демонстрируемые действия влекут или с высокой долей вероятности могут повлечь наступление тяжких и особо тяжких последствий (например, смерть человека).

Участниками треш-стримов являются лица, непосредственно осуществляющие унижающие собственное достоинство высказывания и (или) выполняющие в отношении себя подобные действия (персонажи); лица, заказывающие осуществление определенных и конкретных высказываний и (или) действий, которые должен выполнить иной участник проведения прямого эфира (донатеры); лица, инициирующие и организующие трансляцию, осуществляющие передачу заданий, полученных от донатеров, непосредственному исполнителю – персонажу для выполнения

[1] Официальный сайт Совета Федерации Федерального Собрания Российской Федерации. URL: http://council.gov.ru/events/news/122549/?hl=%D1%82%D1%80%D0%B5%D1%88-%D1%81%D1%82%D1%80%D0%B8%D0%BC (дата обращения: 19.12.2020).

(ведущие). Разные варианты треш-стримов допускают соединение нескольких ролей участников. Вместе с тем имеющаяся информация о треш-стримах позволяет говорить о том, что их классическим форматом является обеспечиваемая ведущим трансляция выполнения персонажем заданий, которые дают донатеры. Участие в треш-стримах не всегда имеет добровольный характер.

Таким образом, по сути, опасность связана не только с действиями и высказываниями, в результате которых причиняется различный вред и которые являются наказуемыми в соответствии с уголовным законом и законодательством об административных правонарушениях. В треш-стримах главное – это передача, трансляция аморальных, противоправных высказываний и действий.

Отличительной особенностью современных треш-стримов является их практически абсолютная монетизация. Данное деструктивное социальное антиправовое явление приносит некоторым из его участников материальный доход, который может достигать больших размеров. Выполнение заданий осуществляется после внесения донатерами платы. В виртуальном мире она называется донат и означает пожертвование финансовых ресурсов. При отсутствии правового регулирования работы блогеров в виртуальном пространстве донаты являются перспективным способом заработка. Стабильность и масштабность получения донатов обеспечиваются наличием постоянной аудитории и уникальностью контента. Кроме того, изучение представленной в открытых источниках информации свидетельствует о том, что имеются факты относительно постоянного финансирования некоторых контентмейкеров (участников треш-стримов) для обеспечения возможности постоянного вещания треш-стримов. Материальную выгоду приносит также размещение рекламы. Как правило, речь идет о компаниях-заказчиках, которые осуществляют нелегальную или полулегальную букмекерскую и иную деятельность. Соответственно, стремление заработать и рыночная конкуренция, также присущая виртуальному миру, логично мотивируют контентмейкеров на продажу все более изощренного и тяжелого насилия, унижения и издевательства.

Указанные факты определяют необходимость установления уголовной ответственности за трансляцию высказываний и (или)

действий, имеющих аморальный, асоциальный и (или) противоправный характер, а также финансирование таких трансляций; создания правовых механизмов блокировки контентов, содержащих треш-стримы; противодействия финансированию треш-стримов.

Заслуживает поддержки мнение главы комиссии Совета Федерации по информационной политике и взаимодействию со СМИ А.К. Пушкова о введении законодательного запрета на осуществление треш-стримов[1]. Представляется, что любой контент, содержащий треш-стримы, подлежит немедленной и безусловной блокировке. В связи с этим особое значение приобретает внутренняя политика интернет-платформ по разработке правил поведения пользователей. Например, видеостриминговым сервисом Twitch для зрителей, стримеров и модераторов сервиса введены правила, являющиеся, по сути, внутренним распорядком, устанавливающим детали и особенности пользования сервисом, определенные запреты и наказание за нарушения в виде ограничений и блокировки. В основе этих правил лежат правовые и морально-этические нормы. Так, запрещено разжигать ненависть, проявлять чрезмерную жестокость к людям и животным, пропагандировать или открыто призывать к тирании и жестокому отношению, размещать любые материалы сексуального характера, оглашать личную информацию о человеке без его разрешения[2]. Вместе с тем эффективность реализации этих правил связана с осуществлением постоянного и действенного контроля за их выполнением, применением адекватных мер реагирования на нарушения с возможностью не только полной, но и постоянной блокировки контента, а также обеспечением условий невозможности создания аналогичных контентов теми же лицами.

Что касается вопросов финансирования треш-стримов, то отметим следующее. Используемые разными видеостриминговыми платформами сервисы оплаты имеют открытый и доступный характер. Это позволяет не только перевести деньги, но и контролировать заинтересованным органам движение средств по счету с предоставлением права и обязанности блокировки воз-

---

[1] URL: https://rg.ru/2020/12/16/pushkov-predlozhil-zapretit-zakonodatelno-zapretit-tresh-strimy.html (дата обращения: 19.01.2021).

[2] URL: https://help-twitch.com/pravila-twitch.html (дата обращения: 14.01.2021).

можности оплаты такого продукта. Кроме того, следует учитывать, что именно действия донатеров по финансированию трешстримов являются стимулом, причиной трансляций аморальных и (или) противоправных высказываний и действий в информационно-телекоммуникационных сетях. Данные действия донатеров, безусловно, должны иметь правовую оценку государства в виде установления уголовной и иной ответственности.

Вместе с тем предлагаемые меры нормативно-правового характера, как и принятые в сфере информационно-коммуникационных технологий нормативные правовые акты, обусловлены необходимостью решения образовавшихся проблем и устранения реальной общественной опасности. В целях же обеспечения законности и правопорядка на длительную перспективу особенно актуально опережающее правовое регулирование общественных отношений в области развития и использования новейших информационных, коммуникационных и иных технологий.

Динамичность образования различных способов и сфер использования технологий, а также появления и применения ранее неизвестных технологий определяет широкое внедрение новых для правовой практики понятий и терминов, относящихся не только к правовым, но и к иным наукам, например кибернетике, и в частности теории информации. Это обусловливает необходимость комплексной законотворческой работы с привлечением специалистов разных областей знаний. Особое значение должно придаваться унифицированности и универсальности определения понятий и терминов, что обеспечит их безусловное правоприменение, в том числе при реализации уголовно-правовых, уголовно-процессуальных норм защиты, даже при появлении новых или трансформации существующих видов технологий и способов их использования. Организация и проведение комплексных научных исследований в рассматриваемой сфере должны способствовать разработке наиболее эффективных правовых мер обеспечения законности, соблюдения прав и свобод человека и гражданина.

Е.Б. Серова,
заведующий кафедрой уголовного процесса и криминалистики Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации, кандидат юридических наук, доцент

Некоторые проблемы доказывания по делам о преступлениях, совершенных с использованием высоких технологий

Современный этап развития общества характеризуется повсеместным развитием компьютерной техники и компьютерных технологий, включая созданные с их использованием компьютерные сети (социальные, файлообменные, локальные и пр.), которые можно с известной долей условности объединить понятием «высокие технологии». Несмотря на позитивное значение развития и использования высоких технологий, они все чаще становятся предметом интереса со стороны криминала и все шире используются в противоправных целях. Фактически при помощи персонального компьютера и современных информационно-коммуникационных технологий могут совершаться практически любые преступления.

Использование высоких технологий закономерно влечет за собой формирование новой обстановки совершения преступления (информационной среды), новых способов совершения преступления, предполагающих использование имеющихся и модифицированных компьютеров, программного обеспечения и сетевых технологий, а также нетривиальных технических решений. Компьютерная техника как комплексное понятие, включающее в себя компьютеры, компьютерные технологии и программное обеспечение, приобретает двуединый характер. Она может выступать и как предмет преступного посягательства, и как новое орудие преступления.

Логическим следствием этого является появление новых следов преступления, механизм формирования которых подвержен собственным закономерностям, предопределяющим основ-

ные особенности процесса доказывания по делам о преступлениях, совершенных с использованием высоких технологий. Характерными их особенностями являются машиночитаемость, нестойкость, отсутствие или трудное выявление информации о следообразующем объекте, что делает затруднительной или невозможной его идентификацию. Различные авторы называют данные следы виртуальными[1] (на наш взгляд, наиболее оптимальное предложение), электронно-цифровыми[2] и т.п. Отсутствует единство мнения и относительно природы указанных следов. Несмотря на указанные особенности виртуальных следов, они несут значимую доказательственную информацию, а потому должны активно выявляться и использоваться в ходе расследования. Однако правоприменитель в своей деятельности должен учитывать особенности следообразования и избегать традиционных подходов в доказывании.

Виртуальные следы, в частности, могут быть обнаружены в электронных документах, содержащих информацию о преступлении (так называемых электронных доказательствах), хранящихся на различных гаджетах, дисках, картах памяти, на серверах провайдеров, в облачных хранилищах и т.д. В пространственном отношении они могут быть значительно удалены друг от друга и не всегда связаны с местом нахождения лиц, привлекаемых к уголовной ответственности. Данные особенности следообразования предполагают необходимость взаимодействия лица, осуществляющего предварительное расследование, с Роскомнадзором, операторами связи и интернет-провайдерами.

Поскольку Интернет облегчает коммуникацию лиц, находящихся не только в различных регионах страны, но и в различных государствах, и обеспечивает возможность реализации противоправных действий вне зависимости от нахождения на конкретной территории, преступления, совершаемые с его помощью, нередко носят трансграничный характер, что требует активного взаимодействия правоохранительных органов России на международном уровне.

---

[1] См.: *Мещеряков В.А.* Преступления в сфере компьютерной информации: правовой и криминалистический аспект: монография. Воронеж: Изд-во Воронеж. гос. ун-та, 2001 и др.

[2] *Поляков В.В., Лапин С.А.* Средства совершения компьютерных преступлений // Докл. Том. гос. ун-та систем управления и радиоэлектроники. 2014. № 2 (32). С. 162–163.

Информация о преступлении, совершенном с использованием высоких технологий, может поступить из разных источников. Как отмечают исследователи, «обнаружить запрещенный контент, вредоносные программы, факты нарушения авторских прав на программы для ЭВМ и базы данных, видеоролики с записями совершенных преступлений и других преступных проявлений может неопределенный круг лиц»[1]. Наиболее типичными источниками информации о преступлении рассматриваемой группы, с нашей точки зрения, являются:

заявления граждан, которые непосредственно обнаружили информацию криминального содержания в процессе использования компьютерной техники в личных целях;

сообщения средств массовой информации и общественных организаций;

результаты оперативно-розыскной деятельности по выявлению и оценке электронной информации криминального содержания, а также по установлению мест ее хранения (сайтов, баз данных и пр.)[2].

Вне зависимости от того, из какого источника поступила информация о преступлении, она требует процессуальной проверки, в ходе которой начинается процесс доказывания события преступления и иных обстоятельств, входящих в предмет доказывания по уголовному делу. Особое внимание в ходе такой проверки уделяется изъятию, исследованию и оценке информации, хранящейся на различных носителях (электронных и бумажных), и компьютерному оборудованию. Материалы проверки должны содержать результаты оперативно-розыскной деятельности, представленные следователю в установленном порядке, протоколы осмотров (места происшествия, предметов, документов), изъятия образцов для сравнительного исследования, объяснения за-

---

[1] *Кириллова Н.П., Кушниренко С.П.* Проблемы осуществления уголовного преследования по делам о преступлениях, совершаемых в сфере высоких информационных технологий // Правоведение. 2013. № 3.

[2] См.: *Бедарев К.В.* К вопросу о мониторинге сети Интернет при выявлении преступлений экстремистской направленности // Бизнес. Образование. Право. Вестн. Волгоград. ин-та бизнеса. 2018. № 2 (43); *Середнев В.А.* Интернет как эффективное сетевое пространство для проведения оперативно-разыскных мероприятий // Вопр. соврем. юриспруденции: сб. ст. по материалам LX междунар. науч.-практ. конф. № 4(55). Новосибирск: СибАК, 2016 и др.

явителя и иных лиц, материалы исследований носителей информации или заключения соответствующих судебных экспертиз и т.п.[1] При этом особо отметим значение для достижения целей доказывания организации и осуществления взаимодействия следователя и подразделений органов, осуществляющих оперативно-розыскную деятельность, и координации усилий правоохранительных органов с государственными и негосударственными структурами, специализирующимися на обеспечении безопасности в сфере телекоммуникаций и компьютерной информации[2].

Важное место в системе доказательств по делам о преступлениях иследуемой группы занимает протокол осмотра места происшествия, который должен содержать сведения о компьютере и содержащейся на нем информации, имеющей отношение к делу. В ходе осмотра необходимо изъять (или скопировать) информацию на электронных носителях, сделать скриншоты, осуществить фото- и видеофиксацию хода и результатов данного следственного действия. Следует подчеркнуть, что осмотр проводится с обязательным участием специалиста.

Еще один протокол, имеющий важное доказательственное значение, – протокол осмотра электронных средств связи, носителей информации и компьютерной техники (смартфонов, ноутбуков, планшетов и т.п.), который должен содержать описание идентификационных признаков устройства, сведения об установленных на нем приложениях и ином программном обеспечении, о файлах, имеющих значение для дела. Осмотр указанных объектов также должен быть проведен с участием специалиста в области компьютерной техники, который помогает следователю установить тип, программное обеспечение устройства, средства его защиты от несанкционированного доступа.

В заключение обратим внимание на еще одну важную составляющую процесса доказывания по делам о преступлениях исследуемой группы – необходимость использования знаний

---

[1] См., например: *Черепанова Л.В.* Хищение денежных средств с помощью системы Интернет: преступления новые, проблемы доказывания старые // Актуал. проблемы борьбы с преступлениями и иными правонарушениями. 2016. № 16-1.

[2] *Антонов И.О., Шалимов А.Н.* Актуальные проблемы расследования мошенничества с использованием компьютерной информации // Уч. зап. Казан. ун-та. Сер.: Гуманитар. науки. 2015. Т. 157. Кн. 6.

специалистов в области компьютерной техники и информационных технологий. Предметом исследования с помощью специалиста может быть компьютерная информация, хранящаяся непосредственно на компьютере, флеш-картах, картах памяти, сервере провайдера интернет-услуг, облачных хранилищах и т.д. Отметим здесь важность процессуальных форм использования специальных знаний, таких как участие специалиста в производстве следственных действий и производство судебных экспертиз. Менее распространенное на практике заключение специалиста также может быть использовано в качестве доказательства по уголовному делу. Помимо этого специалисты могут привлекаться для оказания помощи следователю при подготовке следственных действий, для формулирования вопросов эксперту, разъяснения технических аспектов механизма преступления и пр. В этом случае речь идет о непроцессуальных формах использования специальных знаний.

В.Н. Шиханов,
доцент кафедры уголовно-правовых дисциплин Иркутского юридического института (филиала) Университета прокуратуры Российской Федерации,
кандидат юридических наук,
доцент

Уголовная статистика: подспорье в противодействии преступности или кладбище данных?

О важности достоверной и полной статистической информации о состоянии преступности и результатах борьбы с ней сказано очень много. Мониторинг и прогнозирование криминальной обстановки, планирование правоохранительной работы и профилактики преступности, криминологическое обоснование уголовно-правовых норм и корректировки уголовного закона, оценка эффективности – все это в российской специальной литературе и

практике управления традиционно опирается на уголовную статистику. Неслучайно в настоящее время вопросу развития системы единого учета преступлений и достоверности статистической отчетности уделяется серьезное внимание[1].

Вместе с тем результаты включенного наблюдения, анализа служебных документов правоохранительных органов (открытого характера), а также специальной литературы позволяют обозначить ряд вопросов, требующих серьезного обсуждения.

С 2012 г. проделана большая работа по обеспечению полноты и достоверности собираемой статистической информации. Это касается и порочной практики разбиения единого продолжаемого преступления на эпизоды, и искажения сведений о рецидиве, о состоянии опьянения, о причиненном и возмещенном ущербе, о совершении преступления в общественных местах, вообще о движении уголовных дел и т.д. В то же время точность принятия решений в области уголовной политики, а по многим вопросам и в сфере управления правоохранительными органами не изменилась.

Если мы обратим внимание на содержание пояснительных записок к законопроектам (которые были приняты), то обнаружим, что данные уголовной статистики далеко не всегда являются обязательным атрибутом обоснования уголовно-политического решения. Если же эти данные используются, то качество работы с ними не соответствует уровню даже старших курсов юридических вузов. Нередко статистика никак не подтверждает тезис субъекта законодательной инициативы[2]. Во многом это касается и организационно-управленческих решений в органах исполнительной власти.

Более того, в научной литературе спрос на полную и достоверную уголовную статистику не особенно высок[3]. Например, большинство вопросов уголовного и уголовно-исполнительного

---

[1] Статья 51 Федерального закона от 17.01.1992 № 2202-I «О прокуратуре Российской Федерации».

[2] *Давыдова К.В., Разогреева А.М.* Аналитика криминализации: глубина против поверхности (на примере законов «о пьяных за рулем») // Право и политика. 2015. № 10 (190). С. 1387.

[3] *Лунеев В.В.* Проблемы науки о борьбе с преступностью // Пенитенциарная наука (Вестн. Волгоград. ин-та экономики и права ФСИН России). 2008. № 2. С. 4, 7, 10, 15–18; *Его же*. Истоки и пороки российского уголовного законотворчества. М.: Юрлитинформ, 2014. С. 8–11.

права успешно решаются логико-юридическими методами, а чтобы констатировать масштаб какой-то проблемы (применения статьи Общей или Особенной части УК РФ), исследователям обычно требуются статистические данные за пять предшествующих лет.

Для решения этих задач достаточно всего нескольких разделов форм федерального статистического наблюдения с информацией о количестве зарегистрированных, расследованных преступлений и количестве лиц, привлеченных к ответственности, с разбивкой по статьям УК РФ, по субъектам Российской Федерации и нескольким актуальным направлениям статистического учета, которые объединяют разные статьи Особенной части УК РФ (коррупция, экстремизм, экономика).

Теперь необходимо обратить внимание на объем работы по сбору и обработке данных уголовной статистики. Если до передачи функций правовой статистики в органы прокуратуры объем учитываемых единиц информации по одному преступлению доходил до 5000[1], то теперь он увеличен существенно, в том числе в рамках развития Государственной автоматизированной системы правовой статистики. Также необходимо учесть ту колоссальную работу, которая проводится в рамках борьбы с непреднамеренными и целенаправленными искажениями статистической информации.

Здесь и возникает диссонанс: сегодня всеми возможными пользователями уголовной статистики реально используется примерно 10% собираемой информации. В аналитических обзорах Генеральной прокуратуры Российской Федерации и МВД России результаты осмысления собранной статистики представлены подробнее, однако следы этого анализа в дальнейших работах практически не прослеживаются. Получается, что правоохранительные органы и органы прокуратуры, работая в рамках ненормированного рабочего времени, заняты формированием информации ради ее формирования, борются за достоверность ради самой достоверности. По всей видимости, мы имеем дело с феноменом, который социологи метко назвали кладбище данных.

---

[1] *Лунеев В.В.* Курс мировой и российской криминологии: учебник: в 2 т. Т. I. Общая часть. М.: Юрайт, 2011. С. 257.

Можно возразить, и возразят: сейчас развиваются технологии обработки больших объемов информации, в том числе моделирующие искусственный интеллект (нейросети), а потому на основе такого большого объема собираемой информации мы сможем формировать более сложные отчеты и сделать более точные выводы.

Нисколько не сомневаясь в современных возможностях BigData, позволим заметить, что эти методы всегда исходят из некоторой исследовательской парадигмы. Иными словами, разработчик нейросети связан параметрами того, где и что именно нужно искать, а также содержанием базы данных. А это в свою очередь связано с теми вопросами, на которые в статистической карточке (документе первичного учета) отвечает следователь, дознаватель, прокурор.

Вопросы в современных статкарточках исходят из таких представлений о преступности, многие из которых были в науке переосмыслены либо не являются догмой. Если уголовная статистика нужна для науки, то следует обратиться к очевидным положениям: ученый должен иметь возможность повернуть эмпирические данные под разными углами, построить гипотезу и проверить ее. Простейший пример – современные справочники о социальном и должностном положении обвиняемого, которые далеки от достижений социологии и структуры российского общества. В итоге портреты преступников, традиционно формируемые на основании собираемых статистических данных, выглядят курьезно и не оказывают помощи ни науке, ни практике, а среди обывателей нередко вызывают едкие комментарии. Заметим, что в соответствии с ч. 1 ст. 9 Федерального закона от 29.11.2007 № 282-ФЗ «Об официальном статистическом учете и системе государственной статистики в Российской Федерации» первичные статистические данные, включенные в федеральные формы статистического наблюдения (официальный государственный статистический отчет), не могут быть предоставлены кому-либо, а потому даже ученые de jure должны довольствоваться готовыми статистическими отчетами по утвержденным официальным формам.

В этом отношении гораздо более интересными оказываются массивы не статистики, собранной таким образом, а самих про-

цессуальных решений, в том числе приговоров. Методы работы с BigData позволяют получить из них многое из того, что сопоставимо с собираемой уголовной статистикой, и даже гораздо больше: вплоть до уклонов судебной практики. Быть может, продуктивнее собирать не статистику, а процессуальные документы?

Но главная проблема с разработкой методов анализа собираемой статистической информации состоит в другом: имеется ли в уголовно-политической плоскости, а также в вопросах управления правоохранительными органами дефицит точной информации, сформированной на базе уголовной статистики с использованием технологий такого анализа? Готовы ли политики отодвинуть свои интересы и представления о методах принятия решения на второй план, уступив место строгой и научно выверенной уголовной статистике?

Здесь уместно обратить внимание на концепцию формирования статистической отчетности. В момент ее зарождения и становления было совершенно логичным создавать отдельные информационно-справочные документы (статкарточки, документы первичного учета и другие наименования принципиально схожих по функции носителей): не было ни обобщенных баз текстов принятых процессуальных решений, ни их машиночитаемых вариантов разметки, ни способов их учета, обработки и анализа. Статистические карточки должны были стать информационной выжимкой юридически значимой информации, и вот ее постепенно учились обрабатывать в автоматизированном контуре.

Почему же сейчас, когда имеется принципиальная возможность использования электронного документооборота и изъятия информации прямо из процессуального документа, нам требуется составлять параллельную реальность из статкарточек. Если сейчас имеются возможности автоматического сопоставления информации, проверки логики в самих статдокументах, межбазовых сверок, то зачем давать возможности следователю или дознавателю допустить ошибки, а обязанности по их выявлению и пресечению возлагать на прокурора? Не проще ли включить этот контроль в процесс формирования агрегированных (обезличенных) статистических сведений о преступлении и уголовном деле?

Рационально ли такое использование сил и средств, которое мы наблюдаем сегодня при формировании этого кладбища данных? Во многих странах используются гораздо меньшие по объему данные уголовной статистики, и сложно утверждать, что у наших дальних и ближних соседей из-за этого в области уголовной политики, а также управления правоохранительными органами дела идут из рук вон плохо. Очевидно, нюанс в чем-то другом.

Российскими и зарубежными специалистами давно выявлены сильные и слабые стороны уголовной (в нашем случае – полицейской) статистики[1], в том числе подверженность искажениям в угоду ведомственным интересам и неизбежная однобокость. Прогнозы преступности только на ее основе – занятие возможное, но очень скользкое.

Проблема латентности преступлений не снята и принципиально не может быть преодолена работой по обеспечению полноты и достоверности статистической информации, предоставляемой органами дознания и предварительного расследования. Методы преодоления этой проблемы также известны и проверены[2]. Ведущим из них является регулярное проведение обзоров виктимизации. Эта работа требует усилий и финансирования, однако вектор развития отечественной эмпирической криминологической базы не учел международного опыта и мнения отечественных специалистов.

Обвинять субъектов принятия организационных и уголовно-политических решений в недальновидности и глупости – это простой, но непродуктивный ход, который в итоге скрывает от исследователя строгую логику развития общественных отношений. Поэтому более точным видится другой вывод: уголовная статистика в нынешнем и ожидаемом виде не рассматривается как эмпирическая база, отражающая реальные криминальные (и смежные) процессы в нашем обществе. Если бы нужна была точная информация такого плана, то были бы выбраны иные решения.

---

[1] *Шнайдер Г.Й.* Криминология / пер. с нем. Ю.А. Неподаева; под общ. ред. и с предисл. Л.О. Иванова. М.: Прогресс-Универс, 1994. С. 112–123 и др.

[2] *Шнайдер Г.Й.* Указ. соч. С. 124–146; *Криминология* / под ред. Дж. Ф. Шелли; пер. с англ. СПб.: Питер, 2003. С. 101–131; *Криминология* / под общ. ред. А.И. Долговой, 4-е изд., перераб. и доп. М.: Норма; ИНФРА-М, 2013. С. 117–122, 137–151 и др.

Вернемся к тезису о том, что уголовная статистика не используется в реальной политике как реальный индикатор криминальных процессов. По всей видимости, она явилась частью менеджмента управления, выступая индикатором отношений целеполагания и распределения бюджетных ассигнований внутри правоохранительного блока[1].

Увы, правоохранительные органы, а также органы прокуратуры в настоящее время находятся в незавидном положении: отказаться от трудоемкой работы по сбору статистической информации они не смогут, тем более что в развитие ГАС ПС вложены серьезные ресурсы.

Эта ситуация не является, однако, и безнадежной: необходимы обсуждение имеющихся проблем и корректировка работы таким образом, чтобы собираемая информация приносила существенную пользу самим правоохранительным органам в их повседневной деятельности, освобождая от рутинных операций и предоставляя мощные аналитические инструменты. Но и в этом качестве уголовная статистика не сможет претендовать на серьезную эмпирическую базу для настоящей науки. Повысить ее научную полезность можно, предоставив доступ к собираемой базе данных хотя бы НИИ или оператору, который по запросам исследователей смог бы применять современные методы их обработки, анализа. Полагаем, такие возможности в рамках цифровой трансформации органов прокуратуры (с позиции направления «Среда доверия») можно развивать в рамках портала crimestat.ru.

---

[1] *Ефименко М.О., Скоморохов Р.В., Шиханов В.Н.* Криминологическая теория и практика в организации ведомственного контроля за достоверностью уголовной статистики. М.: Волтерс Клувер, 2010. С. 135–200.

М.В. Шкеле,
доцент кафедры уголовного права
Санкт-Петербургского университета
МВД России, кандидат юридических
наук, доцент

Н.И. Кузнецова,
старший преподаватель
кафедры уголовного права
Санкт-Петербургского университета
МВД России, кандидат юридических
наук

Ресурсы информационно-коммуникационных технологий в сфере противодействия экологической преступности

Одним из наиболее перспективных направлений противодействия экологическим преступлениям в Российской Федерации, а также совершенствования деятельности правоохранительных органов следует признать возможности использования информационно-коммуникационных технологий. Основу развития информационного общества в России заложил Указ Президента Российской Федерации от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы». Следует остановиться на понятии информационно-коммуникационных технологий (информационных технологий). Согласно ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» к информационным технологиям относятся процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Во-первых, использование информационных технологий может значительно снизить уровень латентности экологической преступности. Это тем более важно, что, по оценкам экспертов, латентность экологической преступности считается одной из са-

мых высоких[1]. Информационно-коммуникационные технологии способствуют внедрению новых способов обнаружения, фиксации и предупреждения нарушений экологического законодательства[2]. При помощи информационных технологий могут осуществляться контроль за соблюдением режима особо охраняемых природных территорий, контроль за вырубкой леса, контроль за уровнем загрязнения воздуха, воды, почв, фиксироваться случаи браконьерства, может проводиться наблюдение за несанкционированными мусорными полигонами, возникновениями пожаров, наводнений и др. Например, применение акустической системы наблюдения фиксирует звук выстрелов оружия. Это может быть использовано для предупреждения случаев незаконной охоты.

Использование видеоловушек доказало свою эффективность и применяется для привлечения виновных к уголовной ответственности. Так, шесть лет лишения свободы в колонии общего режима получил гр-н С., задержанный осенью 2018 г. во время рейда. Доказательственная база по делу была сформирована с применением фотоловушек. «Задержанию браконьера предшествовало несколько месяцев кропотливой работы. Первый снимок постороннего зафиксировала фотоловушка в марте 2018 года. Благодаря фотоловушке личность нарушителя установили и выяснили, что это житель села Верхнеусинское гр-н С. Как только появилась достоверная информация, что гр-н С. отправился в заповедник, сотрудники Саяно-Шушенского заповедника обратились к коллегам и организовали совместное патрулирование в труднодоступной местности. В результате браконьер был задержан и доставлен в ОП МО МВД России «Шушенский», – пишет пресс-служба Саяно-Шушенского заповедника[3].

В целях противодействия экологическим преступлениям следует учитывать и данные о том, что в настоящее время сеть «Интернет» является самой популярной платформой для нелегальной торговли дикими животными, в том числе занесенными в

---

[1] *Лопашенко Н.А.* Экологические преступления: комментарий к главе 26 УК РФ. СПб.: Юрид. центр Пресс, 2002. С. 6.

[2] *Дицевич Я.Б.* Информационные технологии в природоохранной деятельности органов прокуратуры // Законность. 2020. № 10 (1032).

[3] *Браконьера* осудили на шесть лет. Криминальные новости Республики Хакасия. URL: https://tvrts.ru/index.php/rts-novosti/kriminal-i-proisshestviya (дата обращения: 18.01.2021).

Красную книгу Российской Федерации и охраняемыми международными договорами, а также их частями и дериватами. В 2019 г. на XVI конгрессе немецких, австрийских и швейцарских криминологов в Вене отмечалось в одном из докладов, что средства сети «Интернет» позволяют осуществлять продажи анонимно и напрямую покупателю. Указывалось, что, например, в 2018 г. торговля охраняемыми черепахами в Китай происходила «на самом видном месте»[1]. В связи с этим представляется, что мониторинг интернет-ресурсов с целью выявления незаконной торговли охраняемыми животными, их частями и дериватами становится важным направлением в противодействии экологическим преступлениям.

Во-вторых, использование информационных технологий должно быть нацелено на совершенствование информационного обеспечения деятельности сотрудников правоохранительных органов по предупреждению, раскрытию и расследованию преступлений. Наиболее эффективными следует признать три типа информационных систем:

1) регистрационные;

2) справочно-информационные;

3) аналитические[2].

Могут создаваться базы цифрового контента – фото и видео с мест происшествия, видео с мест проведения следственных действий, базы видео, полученных от использования дронов, видеоархив с улиц населенных пунктов.

В-третьих, применение информационных технологий ведет к экономии средств и времени. Например, видеоконференцсвязь позволяет проводить конференции, совещания, встречи, организовывать межведомственное взаимодействие.

Важным направлением в экономии затрат рабочего времени представляются разработка и использование информационных

---

[1] *Schloenhardt A., Ege G.* Wildlife Trafficking: Criminological, International and Criminal Law Perspectives // Sag, wie hast du's mit der Kriminologie? Die Kriminologie im Gespräch mit ihren Nachbardisziplinen. Band 118 /Hrsg. von Christian Grafl, Monika Stempkowski, Katharina Beclin und Isabel Haider Forum Verlag Godesberg. 2020. S. 114.

[2] *Шавыркин Б.Б., Сиренко Б.Н.* Информационные технологии – эффективное средство борьбы с преступностью // Актуал. проблемы правового, экономического и социально-психологического знания: теория и практика: материалы междунар. науч.-практ. конф. 17 мая 2017 г. Донецк: ООО «Цифровая тип.», 2017. С. 57.

систем, которые за счет искусственного интеллекта способны анализировать большой объем данных на этапе предварительной обработки материалов. Системы искусственного интеллекта применяются при поиске запрещенного контента в сети «Интернет».

Роботизированные системы на основе искусственного интеллекта могут «отсматривать» большие объемы видеоматериалов в поисках признаков противоправной активности человека как ретроспективно в поисках виновного в очередном правонарушении, так и в режиме реального времени. Так, для мониторинга использования лесов применяются спутниковые системы наблюдения. Для оптимизации природоохранной деятельности министерство природных ресурсов, лесного хозяйства и экологии Пермского края разрабатывает такие системы, как «Умный лес» и «Орбитальный надзор». К основным задачам проекта «Умный лес» относятся формирование единого информационного пространства лесного фонда и автоматизация мониторинга спутниковых снимков для выявления незаконных вырубок[1].

Значимую роль в фиксации правонарушений могут сыграть и интернет-приемные правоохранительных органов. Активному и ответственному гражданину не обязательно теперь лично являться в отделение внутренних дел или в прокуратуру, достаточно сделать заявление с использованием доступа в сеть «Интернет», в том числе и с мобильного устройства связи. Предполагается создание доступного специального сервиса, с помощью которого каждый гражданин сможет подать заявление в правоохранительные органы в электронном виде. Этот документ будет заноситься в систему правовой статистики, регистрироваться под уникальным номером и автоматически направляться по подследственности. При этом автор обращения имеет возможность в любой момент навести справку о статусе своего заявления[2].

Перспективным направлением является использование различных мобильных приложений, которые позволяют оптимизировать процессы коммуникации, создавать определенное информационное пространство. Например, в настоящее время разраба-

---

[1] *Калинина Е.* Применение дистанционного мониторинга использования лесов при осуществлении прокурорского надзора // Законность. 2020. № 1. С. 8.

[2] *Капинус О.С.* Цифровизация деятельности органов прокуратуры: настоящее и будущее // Вестн. Акад. Ген. прокуратуры Рос. Федерации. 2018. № 4 (66).

тывается и уже доступна промоверсия мобильного приложения МВД России, в котором реализован сервис подачи онлайн-обращений в подразделение МВД России в регионе нахождения гражданина или в приемную Министерства внутренних дел Российской Федерации[1]. Предназначено приложение для использования любыми пользователями без ограничений.

В научной литературе активно обсуждаются идеи не только оптимизации процесса выявления преступлений, но и внедрения систем искусственного интеллекта в работу правоохранительных органов[2], в том числе при рассмотрении дел об экологических преступлениях[3].

Кроме того, автоматизированные системы мониторинга экологических ресурсов, широкое участие природоохранных общественных организаций и отдельных граждан посредством интернет-обращений, по нашему мнению, способны снизить коррупционные риски в природоохранной деятельности, а также противодействовать преступной халатности должностных лиц. Так, при проверке дистанционного мониторинга лесов была выявлена недостоверная информация в отчетах о патрулировании, что повлекло возбуждение уголовного дела по признакам преступления, предусмотренного ч. 1 ст. 293 УК РФ[4].

Активное задействование информационно-коммуникационных технологий в сфере выявления экологических преступлений, собирания доказательственной базы, реализации правосудия, а также в направлении профилактики экологических правонарушений и в сфере экологического просвещения населения является непременным условием успеха в природоохранной деятельности.

---

[1] Мобильное приложение МВД России. Официальный сайт Министерства внутренних дел Российской Федерации. URL: https://мвд.рф/apps (дата обращения: 09.02.2021).

[2] *Лебедев С.Я.* Цифровой безопасности – цифровой уголовно-правовой ресурс // Криминология: вчера, сегодня, завтра. 2019. № 4 (55).

[3] *Кузнецова Н.И.* О возможности использования «Электронных весов правосудия» при рассмотрении дел об экологических преступлениях // Криминология: вчера, сегодня, завтра. 2019. № 1 (52).

[4] *Калинина Е.* Указ. соч. С. 7.

Н.В. Колесникова,
старший научный сотрудник
Университета прокуратуры
Российской Федерации

О некоторых проблемах государственного единого статистического учета данных о состоянии преступности с использованием ГАС ПС

В последние годы значимость государственной автоматизированной системы правовой статистики (далее – ГАС ПС), опытная эксплуатация которой проводится с 2013 г. в пилотной зоне, возросла в связи с принятием Федерального закона от 27.12.2019 № 487-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам государственного единого статистического учета данных о состоянии преступности, а также о сообщениях о преступлениях, следственной работе, дознании и прокурорском надзоре» (далее – ФЗ-487).

В частности, ФЗ-487 внес существенные изменения в ст. 51 Федерального закона от 17.01.1992 № 2202-I «О прокуратуре Российской Федерации» (далее – Закон о прокуратуре).

Согласно п. 5 ст. 51 Генеральная прокуратура Российской Федерации в целях государственного единого статистического учета осуществляет создание, развитие, ввод в эксплуатацию и обеспечение функционирования ГАС ПС и является ее оператором.

Согласно п. 6 ст. 51 приказы Генерального прокурора Российской Федерации по вопросам государственного единого статистического учета и ГАС ПС, согласованные с федеральными государственными органами и федеральными органами исполнительной власти, обладающими соответствующими первичными статистическими данными, обязательны для исполнения указанными государственными органами.

В 2020 г. вступило в действие Положение о ГАС ПС, утвержденное постановлением Правительства Российской Федерации от 15.12.2020 № 2113, в котором определены принципы создания, функционирования и развития ГАС ПС, ее структура и основные

функции, участники информационного взаимодействия и их полномочия, правила и способы информационного взаимодействия с другими информационными системами, в том числе с использованием единой системы межведомственного электронного взаимодействия, и условия доступа к информации, содержащейся в системе.

В целях реализации ст. 51 Закона о прокуратуре распоряжением заместителя Генерального прокурора Российской Федерации от 11.11.2020 № 622/11р создана межведомственная рабочая группа по разработке нормативных правовых актов в сфере правовой статистики из представителей федеральных государственных органов и федеральных органов исполнительной власти. Целью создания группы являются разработка и совершенствование нормативных правовых актов, регламентирующих порядок ведения государственного единого статистического учета данных о состоянии преступности, о сообщениях о преступлениях, следственной работе, дознании и прокурорском надзоре с учетом ввода в эксплуатацию ГАС ПС в 2022 г. на всей территории Российской Федерации.

В рамках деятельности межведомственной рабочей группы в 2020 г. были разработаны проект межведомственного приказа о порядке организации приема, регистрации и рассмотрения сообщений о преступлениях, проекты приказов Генерального прокурора Российской Федерации о государственном едином статистическом учете данных о состоянии преступности, о сообщениях о преступлениях, следственной работе, дознании, прокурорском надзоре, а также о порядке предоставления первичных статистических данных о состоянии преступности, о сообщениях о преступлениях, следственной работе и дознании в ГАС ПС.

В частности, для обеспечения статистического учета в ГАС ПС разработаны новые документы первичного учета. Они существенно отличаются от документов первичного учета, утвержденных межведомственным приказом Генеральной прокуратуры Российской Федерации, МВД России, МЧС России, Минюста России, ФСБ России, Минэкономразвития России, ФСКН России от 29.12.2005 № 39/1070/1021/253/780/353/399, и используются при проведении опытной эксплуатации.

Перечень статистических карточек в системе ГАС ПС:

учетная карточка на сообщение о преступлении и результаты его рассмотрения (форма «СП»);

регистрационная карточка уголовного дела и материалов проверки сообщения о преступлении (форма «РК»);

статистическая карточка на преступление (форма № 1-ГП);

статистическая карточка на потерпевшего (форма № 2-ГП);

статистическая карточка на причиненный преступлением материальный ущерб и изъятие предметов преступного посягательства, преступной деятельности (форма № 3-ГП);

статистическая карточка на лицо, подозреваемое, обвиняемое в совершении преступления (форма № 4-ГП);

статистическая карточка на лицо, привлеченное к уголовной ответственности по предварительно расследованным преступлениям (форма № 4.1-ГП);

статистическая карточка на движение уголовного дела (форма № 5-ГП);

статистическая карточка на решение прокурора по уголовному делу (форма № 6-ГП);

статистическая карточка на возмещение материального ущерба по уголовному делу (форма № 7-ГП);

статистическая карточка на результаты рассмотрения уголовного дела в суде (форма № 8-ГП).

Для заполнения документов первичного учета Генеральной прокуратурой Российской Федерации ведутся справочники и классификаторы. Справочники и классификаторы подразделяются на три вида:

справочники с литерой «СП», применяемые для заполнения учетной карточки по форме «СП»;

справочники с литерой «ГП», применяемые для заполнения статистических карточек;

справочники с литерой «О» – общие справочники, применяемые для заполнения учетной карточки по форме «СП» и статистических карточек.

Справочники могут быть специализированными, которые разработаны для целей статистического учета данных о зарегистрированных сообщениях о преступлениях и результатах их рассмотрения, о состоянии преступности, следственной работе и до-

знании, а также сформированы на основе общероссийских классификаторов.

В настоящее время проекты документов проходят процедуру согласования, замечания и предложения по ним обсуждаются на заседаниях рабочей группы.

В частности, в межведомственном приказе не урегулирован вопрос о действии должностных лиц при поступлении заявлений и сообщений, не содержащих признаков преступлений. На первоначальном этапе сообщение не всегда возможно однозначно соотнести с признаками преступления или правонарушения (происшествия). Однако разграничение порядка регистрации таких сообщений неизбежно повлечет ведение кроме книги учета сообщений о преступлениях (КУСП) дополнительной учетной формы. Такая практика существовала в системе МВД России и показала свою неэффективность. В настоящее время во всех государственных органах, за исключением МВД России, регистрация сообщений о преступлениях осуществляется в отдельной книге учета. Решением проблемы может стать регистрация в КУСП заявлений и обращений, которые не содержат сведений об обстоятельствах, указывающих на признаки преступления, и не требуют процессуальной проверки в порядке ст. 144, 145 УПК РФ, на основании нормативного правового акта федерального государственного органа, осуществляющего в соответствии с законодательством Российской Федерации полномочия в сфере уголовного судопроизводства.

Не установлен порядок регистрации сообщений о преступлениях и выдачи талона-уведомления заявителю об их принятии в случаях отсутствия возможности использования программного обеспечения (например, сбой в работе, отсутствие электроэнергии и др.). В качестве варианта решения возможно дополнить проект порядком регистрации сообщений о преступлениях в КУСП на бумажном носителе с обязанностью незамедлительного внесения сведений в КУСП в электронном виде при появлении технической возможности.

Возникли определенные проблемы с созданием официальной статистической методологии, которую в соответствии с п. 3 ст. 51 Закона о прокуратуре и Федеральным законом от 29.11.2007 № 282-ФЗ «Об официальном статистическом учете и

системе государственной статистики в Российской Федерации» (далее – ФЗ-282) утверждает Генеральная прокуратура Российской Федерации по согласованию с федеральными государственными органами и федеральными органами исполнительной власти, обладающими соответствующими первичными статистическими данными.

Официальная статистическая методология отражения статистических показателей в документах первичного учета является приложением к Правилам заполнения документов первичного учета, используемых для предоставления первичных статистических данных о состоянии преступности, о сообщениях о преступлениях, следственной работе и дознании в государственную автоматизированную систему правовой статистики, и содержит в себе только понятийный аппарат. Это противоречит ч. 2 ст. 7 ФЗ-282, в которой говорится, что официальная статистическая методология включает в себя методы сбора, контроля, редактирования, сводки и группировки первичных статистических данных и административных данных, составления национальных счетов, оценки точности официальной статистической информации и ее систематизации.

Полагаем, что при дальнейшей проработке нормативных правовых актов, регламентирующих порядок ведения государственного единого статистического учета, целесообразно обеспечить преемственность с действующими нормативными правовыми актами, такими как Типовое положение о едином порядке организации приема, регистрации и проверки сообщений о преступлениях, Положение о едином порядке регистрации уголовных дел и учета преступлений, Инструкция о порядке заполнения и представления учетных документов, утвержденные межведомственным приказом Генеральной прокуратуры Российской Федерации, МВД России, МЧС России, Минюста России, ФСБ России, Минэкономразвития России, ФСКН России от 29.12.2005 № 39/1070/1021/253/780/353/399.

Это важное требование, выполнение которого является необходимым условием проведения комплексного анализа и прогнозирования состояния законности и правопорядка в стране, динамики и структуры преступности.

В проектах приказов есть и чисто технические проблемы.

Например, нуждаются в уточнении корректность кодов элементов справочников и их структура. В частности, справочник «Характеристика группы лиц, в составе которой лицо совершило преступление, и формы соучастия» используется при заполнении реквизитов «Характеристика группы лиц по уровню организации» и «Характеристика группы лиц, в составе которой лицо совершило преступление» статистической карточки формы № 4.1-ГП и содержит две группы с разной размерностью кодов (1 и 4 соответственно). Возможно, стоит разбить справочник на два: «Характеристика группы лиц, в составе которой лицо совершило преступление, по уровню организации» и «Характеристика группы лиц, в составе которой лицо совершило преступление, по форме соучастия».

Кроме того, может вызвать сложности при заполнении статистических карточек имеющая место неоднозначность кодов элементов справочников. Например, в справочнике «Цель въезда в Российскую Федерацию» элементы «трудовой мигрант», «незаконный мигрант», «мигрант-соотечественник – участник государственной программы» являются частными случаями элемента «мигрант».

В статистической карточке формы № 4.1-ГП отсутствует возможность занести данные на лиц без гражданства, так как данной характеристики нет ни в справочнике «Место проживания», ни в справочнике № 4-О «ОКСМ», который содержит перечень стран мира (принят и введен в действие постановлением Госстандарта России от 14.12.2001 № 529-ст). Поэтому представляется возможным создать справочник «Гражданство», подготовленный на основе классификатора «Общероссийский классификатор стран мира (ОКСМ)», и добавить элемент «лицо без гражданства».

В заключение отметим, что выработка согласованной позиции по нормативному регулированию порядка ведения государственного единого статистического учета и функционирования ГАС ПС, в том числе в рамках работы межведомственной рабочей группы, а также дальнейшее совершенствование и принятие нормативных правовых актов является одной из приоритетных задач по данному направлению деятельности прокуратуры.

М.В. Рубцова,
старший научный сотрудник
НИИ Университета прокуратуры
Российской Федерации

Органы прокуратуры в борьбе с киберпреступностью в России

Киберпреступность выступает не только угрозой национальной безопасности Российской Федерации, но и вызовом всему мировому сообществу. В России с 2013 г. число киберпреступлений возросло в 20 раз. К примеру, в 2020 г. зафиксировано увеличение количества тяжких и особо тяжких преступлений на 14%, что связано с ростом количества киберпреступлений. Так, число преступных деяний, совершенных с использованием информационно-коммуникационных технологий, возросло на 73,4%, сети «Интернет» – на 91,3%, средств мобильной связи – на 88,3%[1]. Наиболее заметен рост такого рода преступлений в Москве – 204,3 преступления на 100 тыс. населения, Мурманской области – 200,7, Республике Коми – 191,8. В два раза увеличилось количество преступлений с использованием электронных средств платежа. Здесь лидируют Саратовская (+94,7%), Омская (+136,3%) области и Москва (+113,6%). Наиболее низким кибермошенничество остается в Северо-Кавказском федеральном округе[2]. Как показывает практика, простор для киберпреступлений создает и неограниченный оборот SIM-карт. Случаи приобретения в одни руки, чаще всего по чужим документам, неограниченного числа мобильных телефонных номеров получают все большее распространение. В результате злоумышленники остаются анонимными и безнаказанными. В связи с этим важно усилить механизм взаимодействия с операторами сотовой связи, чтобы оборот SIM-карт был более прозрачным для выявления мошеннических действий, в том числе и самими операторами.

---

[1]URL:https://aif.ru/politics/russia/mvd_rost_chisla_prestupleniy_cherez_internet_v_2020_godu_prevysil_90 (дата обращения: 01.02.2021).
[2]URL: https://riafan.ru/1309488-prestupnost-v-2020-godu-pereshla-v-onlain-rezhim (дата обращения: 13.01.2021).

По оценке Генеральной прокуратуры Российской Федерации, рост мошенничеств с платежными картами связан и с недостатками регламентации защиты банками персональных данных. Борьбе с киберпреступлениями препятствует неопределенность в правовом статусе криптовалюты, поэтому требуется дальнейшая выработка единых подходов к регулированию оборота цифровой валюты на законодательном уровне. Отдельно можно выделить проблему, когда к телефонным мошенничествам и кражам через сеть «Интернет» подключаются заключенные в колониях и СИЗО. Кроме того, появляются новые способы шифрования данных, максимально повышающие анонимность совершаемых действий. Наблюдается широкое распространение криминального использования криптовалют в сфере незаконного оборота наркотиков, коррупции, финансирования организованной преступности, экстремизма и терроризма. Продолжается ежегодный рост компьютерных атак, организаторы которых нередко используют инфраструктуру иностранных государств для попыток взлома информационных систем российских государственных органов, корпораций, крупных банков.

Бесконтактный и быстрый способ совершения таких преступлений делает общество все более уязвимым перед новыми вызовами. При этом правоохранительные органы зачастую оказываются к ним неготовы. Низкая выявляемость и раскрываемость киберпреступлений порождают безнаказанность и чувство вседозволенности, хотя возможности противостоять новым угрозам у правоохранителей имеются. В связи с этим правоохранительным органам было указано на необходимость эффективно отвечать на вызовы в киберпространстве, использовать те же технологии для раскрытия преступлений, предупреждать и прогнозировать их, своевременно устранять правовые пробелы. Государственной Думой принимаются законы в целях противодействия мошенничеству в банковской сфере, в сфере высоких технологий, поскольку страдают самые незащищенные слои населения, которые слабо информированы о работе мобильного банка, мобильных устройств, легко внушаемы, часто подвергаются воздействию извне. Как отмечают эксперты, необходимо постоянно совершенствовать инструментарий борьбы с киберпреступниками.

К 2021 г. планируется разработать платформу для мониторинга фишинговых сайтов и утечек персональных данных.

Имеющиеся проблемы требуют реагирования со стороны всей правоохранительной системы, что обусловливает важность единообразного понимания вызовов и четкой координации работы по их нейтрализации. Необходимы безотлагательные меры по совершенствованию системы профилактики и раннего выявления преступлений, совершенных с использованием IT-технологий и компьютерной информации, по созданию автоматизированных поисковых систем, в том числе на базе существующих, путем расширения функционала по предупреждению и пресечению киберпреступности, а также их интеграции с другими базами данных. Требуется изменить подходы к организации оперативно-розыскной деятельности и предварительного расследования таких фактов. Учитывая специфику их выявления, стремительное распространение криминального использования виртуальных активов, компьютерных атак на критическую информационную инфраструктуру государства, следует внедрять специализацию сотрудников, осуществлять их профессиональный отбор, добиваться устойчивого повышения раскрываемости преступлений, обеспечивать тесное взаимодействие прокуроров, сотрудников оперативных, в том числе технических, служб и следственных органов на этапах выявления данных посягательств и осуществления уголовного преследования виновных лиц, комплексно развивать систему экспертного сопровождения. Учитывая трансграничный характер киберпреступлений, необходимо более эффективно использовать возможности специализированных сетей правоохранительных органов, международного полицейского взаимодействия и сотрудничества в порядке уголовного судопроизводства.

Генеральный прокурор Российской Федерации обратил внимание на необходимость совершенствования действующего законодательства в части расширения признаков преступлений в сфере IT-технологий, введения в процессуальные нормы понятия «электронное доказательство», процедур внесудебной блокировки «зеркал» заблокированных сайтов, а также активного участия в этой работе всех ведомств. «Усилия органов прокуратуры, в свою очередь, будут сосредоточены на повышении эффективно-

сти и качества прокурорского надзора за законностью в сфере безопасного использования информационно-коммуникационных технологий в целях оперативного решения всех стоящих перед нами задач»[1].

Кибербезопасность следует систематически интегрировать в национальные стратегии, управленческие действия на государственном уровне, формируя устойчивое общество, способное противостоять растущим рискам и угрозам в сфере информационных технологий. В соответствии со Стратегией развития информационного общества в Российской Федерации на 2017–2030 годы, утвержденной Указом Президента Российской Федерации от 09.05.2017 № 203, надлежит проводить непрерывный мониторинг и анализ угроз, возникающих в связи с внедрением новых информационных технологий, для своевременного реагирования на них. Коронавирусная инфекция (COVID-19) оказала влияние на увеличение количества киберпреступлений в области торговли контрафактными и некачественными товарами, а также различных видов мошенничества и схем, связанных с организованной преступностью в сфере информационных технологий. В настоящее время требуется единая система борьбы с киберпреступлениями, позволяющая выявлять их еще до обращения потерпевших. Один из вариантов – заключение единого соглашения об электронном обмене информацией между государственными органами и службами при взаимодействии с банками, операторами связи, интернет-провайдерами и иными участниками информационного пространства. Координирующим центром борьбы с IT-преступностью может стать созданный при ФСБ России Национальный координационный центр по компьютерным инцидентам. Либо по примеру международных моделей возможно создание централизованного межведомственного органа по координации их деятельности в круглосуточном режиме, который обладал бы необходимым инструментарием, включая оперативную, следственную и техническую службы, научно-исследовательский центр и центр международного сотрудничества с представительством специалистов всех министерств и ведомств.

[1]URL: https://genproc.gov.ru/smi/news/genproc/news-1880616/ (дата обращения: 28.01.2021).

А.А. Вихляев,
преподаватель кафедры
административной деятельности
ОВД Московского университета
МВД России имени В.Я. Кикотя

К вопросу об использовании сотрудниками полиции личных технических средств при аудио- и видеофиксации противоправного поведения правонарушителей и о допустимости приобщения полученных результатов в качестве доказательств при производстве по делам об административных правонарушениях и в уголовном процессе

В эпоху всеобщей цифровизации современное общество перешло к активному применению средств информационно-технического обеспечения для удовлетворения всех потребностей. Информационно-технические аспекты затрагивают и вопросы правоохранительной деятельности. Применение современных технологических решений в целях предупреждения и пресечения противоправного поведения виновных лиц показало свою состоятельность и существенно помогает в доказывании административно-правовых деликтов и общественно опасных деяний.

Сотрудники полиции являются одними из основных субъектов профилактики, предупреждения и пресечения правонарушений.

В последнее время одним из наиболее обсуждаемых аспектов, затрагивающих специфику предупреждения и пресечения противоправного поведения лиц, является вопрос использования сотрудниками полиции технических средств при фото- и видеофиксации правонарушений и при сопровождении дальнейших действий по получению доказательственных материалов по делам об административных правонарушениях и уголовным делам (фото-, видеосъемка документов, удостоверяющих личность задержанных, особенностей их внешности, состояния одежды, следов противоправных действий и пр.).

Попробуем разобраться в этом вопросе более подробно.

Статьей 11 Федерального закона от 07.02.2011 № 3-ФЗ «О полиции» в качестве основополагающего закреплен принцип,

заключающийся в использовании достижений науки и техники, современных технологий и информационных систем.

В соответствии с ч. 3 указанной статьи полиция использует технические средства, включая средства фиксации, при осуществлении аудиовизуального закрепления и документирования обстоятельств совершения преступлений, административных правонарушений и происшествий. Следует отметить, что под документированием в данном случае понимается запись информации на различных носителях, полученная в соответствии с установленными правилами.

Безусловно, обозначенный принцип в аспекте осуществления информационно-технического сопровождения уголовных дел и производства по делам об административных правонарушениях является бесспорным и в полной мере реализуется должностными лицами органов внутренних дел в административном и уголовном процессе.

Под принципом в данном сегменте понимаются основополагающие идеи или руководящие начала, лежащие в основе полномочий, в то время как при непосредственном предупреждении и пресечении противоправного поведения сотрудники полиции сталкиваются с реализацией основных прав и обязанностей, необходимых для своевременного недопущения повторения противоправных действий со стороны виновных, получения необходимого доказательственного материала и фиксации обстановки на месте совершения противоправных действий. В данном контексте правомочия сотрудника полиции будут выступать в качестве одного из регуляторов общественных отношений.

Права полицейского имеют статус обязательных для исполнения другими лицами и направлены на регулирование общественных отношений в сфере обеспечения правопорядка. Общие, основные и специальные права полиции закреплены в Федеральном законе «О полиции».

Так, в соответствии с ч. 1 ст. 13 Федерального закона полиция имеет право использовать в своей профессиональной деятельности специальные информационные системы, технические и специальные средства, которые не должны причинять вред жизни и здоровью граждан, окружающей среде, а также различные информационные банки данных различного уровня.

Следует заметить, что федеральным законодательством не дается разделение информационно-технических средств, используемых сотрудниками полиции, на служебные и личные.

Отсутствие подобного разграничения на практике трактуется двояко: с одной стороны, в пользу использования сотрудником полиции личных информационно-технических средств при фиксации противоправного поведения виновного лица с последующим представлением полученных сведений в качестве доказательств по уголовным делам и делам об административных правонарушениях, с другой – создает дополнительное поле для обжалования подобных действий и признания доказательств, полученных в результате использования сотрудником полиции личных технических средств, недопустимыми и подлежащими исключению, что в том числе подтверждается и материалами судебной практики. Так, если в случаях дополнительного подкрепления полученных фото-, видео-, аудиоматериалов свидетельскими показаниями в суде подобные материалы являются допустимыми и подтверждают вину лица в инкриминируемом общественно опасном деянии или административно-правовом деликте, то материалы, полученные сотрудником полиции на личные технические средства в отсутствие свидетелей, могут быть признаны недопустимыми и исключены из доказательств по делу.

Имеют место случаи, когда сторона защиты, представляя интересы виновного лица в административном судопроизводстве или уголовном процессе, выступает с ходатайством о признании использования сотрудником полиции личных технических средств в качестве обстоятельств, формально провоцирующих подзащитного на возможное противоправное поведение (полицейский начал снимать правонарушителя, чем спровоцировал его на неповиновение законным требованиям).

В соответствии с ч. 3 ст. 6 Федерального закона «О полиции» сотруднику полиции запрещается подстрекать, склонять, побуждать в прямой или косвенной форме кого-либо к совершению противоправных действий.

В данном случае сторона защиты нередко ссылается на положения Федерального закона от 27.07.2006 № 152-ФЗ «О защите персональных данных», и в частности на п. 1 ч. 1 ст. 6, согласно которому обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку сведений о

нем, а действия виновного лица мотивируются исключительно в качестве потенциальной защиты от действий представителя власти вопреки воле указанного лица.

Согласно действующему законодательству под персональными данными понимается любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных). Таким образом, к указанной информации можно отнести широкий спектр сведений о лице, включая и особенности его внешности, поведения, религиозные воззрения и пр.

Изучение судебной практики показало, что при возникновении сомнений или противоречий при рассмотрении доказательств, полученных сотрудниками полиции на личные технические средства, в большинстве случаев дела об административных правонарушениях и уголовные дела федеральными и мировыми судьями возвращаются прокурорам и должностным лицам органов внутренних дел для устранения противоречий, препятствующих производству по делу.

Формально право сотрудников полиции на фиксацию противоправного поведения лица при пресечении правонарушений законодательством не закреплено, а описанная норма по использованию в деятельности полиции современных технических средств трактуется в нынешней редакции неоднозначно.

Так, в целях разъяснения допустимости запрета на фото-, видео- и аудиофиксацию действий должностных лиц ГИБДД, а также возможностей осуществления фиксации правонарушений с их стороны на любые подручные технические средства МВД России пришлось выпустить официальный информационный бюллетень[1]. При этом право должностных лиц ГИБДД на фиксацию при помощи личных технических средств фактов правонарушений фактически с точки зрения федерального законодательства разобрано не было. Для сотрудников полиции, представляющих иные службы и подразделения органов внутренних дел, подобные разъяснения МВД России официально не выпускались.

[1] Информация МВД России от 01.12.2017 «Госавтоинспекция разъясняет возможность осуществления участниками дорожного движения фотовидеосъемки общения с инспекторами ДПС». URL: http://www.consultant.ru/law/hotdocs/51692.html/ (дата обращения: 20.01.2021).

Кроме того, как можно заключить, официальное разъяснение не является нормативным правовым актом, имеющим обязательную юридическую силу, и с позиции закона рассматриваться не может.

Выход из ситуации видится в законодательном закреплении права сотрудников полиции на использование личных технических средств при аудио- и видеофиксации противоправного поведения правонарушителей и допустимости приобщения полученных результатов в качестве доказательств при производстве по делам об административных правонарушениях и в уголовном процессе в соответствующей статье Федерального закона «О полиции».

Законодательное закрепление указанных полномочий позволит однозначно трактовать действия должностных лиц органов внутренних дел при осуществлении фиксации на личные технические средства противоправного поведения лиц как правомерные, придавая им статус относимых и допустимых доказательств в уголовном процессе и при производстве по делам об административных правонарушениях.

А.Б. Прохоров,
соискатель Санкт-Петербургского
юридического института (филиала)
Университета прокуратуры
Российской Федерации

Некоторые аспекты использования электронных документов в уголовном судопроизводстве

До недавнего времени электронный документооборот практически отсутствовал в деятельности судов и других профессиональных участников уголовного судопроизводства. Прилагательное «электронный» главным образом указывало способ изготовления процессуального документа. Вместе с тем указанное прилагательное никоим образом не отождествлялось с чем-то значимым непосредственно для уголовного судопроизводства. Одновременно с этим вопрос о вхождении электронного документо-

оборота в уголовный процесс не подвергался серьезному теоретическому анализу.

Ситуация изменилась в связи с введением новой редакции гл. 56 УПК РФ в соответствии с Федеральным законом от 23.06.2016 № 220-ФЗ (далее – Федеральный закон № 220-ФЗ). В текст уголовно-процессуального закона было введено понятие электронного документа (ст. 474[1] УПК РФ). Тем самым электронный документ и электронный документооборот стали неотъемлемой частью обязательной уголовно-процессуальной формы. Теперь электронный документооборот охватывает несколько сфер уголовного процесса: подача жалоб и ходатайств в электронном виде, судебные извещения, рассмотрение дела с использованием документов в электронном виде, изготовление и направление судебных актов.

Следует признать, что возможности в электронной сфере создают определенные преимущества для участников уголовного судопроизводства.

Электронные процедуры обусловливают реализацию интересов участников уголовного судопроизводства не только технически. В том смысле, что служат не только техническому воплощению данных интересов (подача ходатайств и жалоб, отслеживание дела и пр.). Можно смело утверждать, подача процессуальных документов в электронной форме гарантирует достоверность процедуры, способствует соблюдению процессуальных сроков.

Всестороннее научное исследование соответствующих вопросов, однако, до настоящего времени не проводилось, некоторые аспекты рассматривались казуально, зачастую на основе устаревшей нормативно-правовой базы.

Научные публикации в обоснование развития электронных полномочий и электронного правосудия как такового появились сравнительно недавно[1].

---

[1] Предметных диссертационных исследований в сфере уголовного процесса мало. Применительно к гражданскому процессу см.: *Василькова С.В.* Электронное правосудие в цивилистическом процессе: автореф. дис. … канд. юрид. наук. Саратов, 2018; применительно к теории построения системы правосудия см.: *Аносов А.В.* Информационно-правовые вопросы формирования электронного правосудия в Российской Федерации: автореф. дис. … канд. юрид. наук. М., 2016.

В связи с указанной научной дискуссией хотелось бы также отметить ряд актуальных вопросов использования электронных документов, имеющих теоретический интерес и практическую значимость.

Итак, детальное внимание должно быть уделено, прежде всего, понятию электронного документа в уголовном судопроизводстве.

Как ясно следует из закона (ст. 474 и 474^1 УПК РФ), понятие электронного документа не является равнозначным понятию документа (процессуального документа), выполненного электронным способом. То есть документу, предварительно набранному в текстовом редакторе компьютерной программы.

Уголовно-процессуальный закон не содержит понятия «электронный документ». При этом в соответствии с п. 1 постановления Пленума Верховного Суда Российской Федерации от 26.12.2017 № 57 (далее – постановление Пленума Верховного Суда РФ № 57) под электронным документом понимается документ, созданный без предварительного документирования на бумажном носителе и подписанный электронной подписью. Понятия «электронный документ» и «электронный образ документа» (электронная копия бумажного документа, заверенная электронной подписью) Верховный Суд Российской Федерации объединил в понятие «документ в электронном виде».

Суды общей юрисдикции используют преимущественно электронные образы своих судебных актов, заверяя эти документы усиленной квалифицированной подписью судьи соответствующего суда. Причем электронная подпись наличествует только у судьи, но не у помощника или секретаря (ст. 244^1, 245 УПК РФ). Соответственно, протоколы судебных заседаний, например, поскольку они подписаны секретарем, не размещаются в личном кабинете стороны (система ГАС «Правосудие»).

Форма электронного документооборота посредством подачи образов электронных документов наиболее распространена в адвокатской практике.

Органы предварительного расследования и органы прокуратуры не используют документы в электронном виде. В органах прокуратуры не регламентирован порядок использования электронной подписи для соответствующих целей. В органах СК Рос-

сии, МВД России, ФССП России и ФСБ России локальное нормативно-правовое регулирование данных вопросов также отсутствует.

Представляется, что под процессуальными документами, поданными в форме электронного документа согласно ст. 474^1 УПК РФ, следует понимать как непосредственно электронные документы, так и электронные образы бумажных документов. К такому выводу приходим, анализируя одновременно с законом положения подп. 3.4.1, 3.4.2 Порядка подачи в федеральные суды общей юрисдикции документов в электронном виде, в том числе в форме электронного документа, утвержденного приказом Судебного департамента при Верховном Суде Российской Федерации от 27.12.2016 № 251 (далее – Порядок подачи документов).

Данный порядок не предусматривает никаких различий в плане юридической силы соответствующих электронных типов документов.

Следует определиться также с законодательством, регулирующим указанную сферу процессуальных отношений. Обращение в суд в электронном виде в рамках уголовного судопроизводства требует соблюдения определенных критериев. Данные критерии (важнейший из них – вид используемой электронной подписи) установлены не только УПК РФ.

На основании ст. 2 Федерального закона № 220-ФЗ Федеральный закон от 18.12.2001 № 177-ФЗ «О введении в действие Уголовно-процессуального кодекса Российской Федерации» (далее – Федеральный закон № 177-ФЗ) дополнен ст. 12^2. Согласно данной норме порядок заполнения электронных форм для подачи электронных документов определяется Верховным Судом Российской Федерации и Судебным департаментом при Верховном Суде Российской Федерации в пределах установленных полномочий. Теми же инстанциями устанавливаются «иные требования, связанные с использованием электронных документов» в уголовном процессе (абз. 2 ст. 12^2 Федерального закона № 177-ФЗ).

Как указано в ч. 1 ст. 474^1 УПК РФ, электронный документ должен быть подписан электронной подписью «в соответствии с требованиями законодательства Российской Федерации». Законом, регулирующим сферу применения электронно-цифровой подписи,

является Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи» (далее – Федеральный закон № 63-ФЗ).

В частности, Федеральный закон № 63-ФЗ устанавливает требования для простой и усиленной квалифицированной электронной подписи (ч. 4 ст. 5), указывает отдельные случаи их применения (ст. 9, 19 и пр.).

С учетом указанного правового регулирования, в соответствии с п. 3.4.1 Порядка подачи документов электронный документ (обращение) должен быть подписан (электронный образ документа – заверен) именно усиленной квалифицированной электронной подписью.

Исходя из существующей модели регулирования в уголовном судопроизводстве все документы требуют усиленной квалифицированной подписи.

В связи с этим необходимо отметить также следующее.

Во-первых, нормы ч. 1 ст. 474^1 УПК РФ и ст. 12^2 Федерального закона № 177-ФЗ сконструированы неудачно. Исходя из буквального толкования данных норм трудно однозначно ответить на вопрос, каким способом устанавливаются требования к виду электронной подписи, используемой для подачи обращений в суд. Кто принимает соответствующий порядок: федеральный законодатель или Верховный Суд Российской Федерации с Судебным департаментом при данном суде.

Во-вторых, на наш взгляд, имеется расхождение между законотворческой традицией и нормативным регулированием, воплощенным Федеральным законом № 220-ФЗ с его дополнениями к УПК РФ и вводному закону.

Так, в соответствии с ч. 1 ст. 1 УПК РФ порядок уголовного судопроизводства на территории Российской Федерации устанавливается данным кодексом, основанным исключительно на Конституции Российской Федерации. Поскольку электронная подпись, как и обычная подпись, является обязательной частью документа (например, подпись под апелляционной жалобой (п. 6 ч. 1 ст. 389^6 УПК РФ), вид электронной подписи (усиленный или простой) должен быть указан в тексте уголовно-процессуального закона. То есть отсылочная конструкция ч. 1 ст. 474^1 УПК РФ вряд ли является приемлемой с учетом традиции правового регулирования анализируемой сферы процессуальных отношений.

Кроме того, требует серьезного научного осмысления делегирование федеральным законодателем своих прав указанным судебным инстанциям (ст. 12^2 Федерального закона № 177-ФЗ) в части установления правил электронного документооборота как части уголовного судопроизводства. Этот шаг может иметь самые широкие последствия, которые, возможно, не до конца просчитаны федеральным законодателем.

Обилие отсылочных и бланкетных норм может привести к росту противоречий правового регулирования.

Вероятно, приведенные особенности толкования законов обусловлены отсутствием четкого понятия электронного документа в УПК РФ. Ситуация осложняется отсутствием единой нормативной концепции использования процессуальных документов в электронном виде. Но при любых обстоятельствах указанная проблематика требует дальнейшего обсуждения. Также представляется, что без решения указанных вопросов об основных дефинициях не будет найден путь к решению прикладных задач, например по использованию электронной формы уголовного дела[1].

Необходимо также отметить, изготовление усиленной квалифицированной электронной подписи требует денежных затрат. При этом, например, адвокаты могут предъявлять документы, подтверждающие расходы на изготовление усиленной электронной подписи, в налоговый орган для предоставления профессионального налогового вычета.

Вместе с тем в целях более широкого применения цифровых возможностей следует рассмотреть идею покрытия соответствующих затрат адвоката-защитника на изготовление цифровой подписи за счет бюджета. Например, это возможно в рамках государственной программы по аналогии с действовавшей государственной программой Российской Федерации «Юстиция» (2013–2020 гг.). Одновременно следует распространить опыт использования электронных документов повсеместно на правоохранительные органы, что с очевидностью позволит экономить время, силы работников и материальные ресурсы.

---

[1] См. подробнее: *Макарова О.В.* Совершенствование судопроизводства путем внедрения электронной формы уголовного дела // Журн. рос. права. 2019. № 2 (266).

М.В. Винокуров,
аспирант Университета прокуратуры Российской Федерации, помощник прокурора Куйбышевского района г. Иркутска

Эффективность применения цифровых технологий в борьбе с фальсификацией лекарственных средств

Лекарственные средства являются наиболее применяемым видом борьбы с болезнями. Вылечиться в домашних условиях без применения лекарств невозможно. Принимать лекарства нужно обязательно, чтобы получить наилучший возможный эффект от лечения[1]. Даже попадая в больницу с самыми тяжелыми заболеваниями, в первую очередь врачи пытаются прибегнуть к лечению при помощи лекарственных средств и только в крайнем случае к проведению операции.

Роль лекарственных средств в жизни современного общества безусловно высока. Но встречаются ситуации, в которых приобретенное лекарство не дает необходимого результата. Такое возможно в результате покупки фальсифицированных лекарств.

Поскольку жизнь и здоровье являются высшей ценностью, их сохранение, следовательно, и качество лекарственной продукции являются значимой задачей государства.

Государственными органами разрабатывается ряд мероприятий, направленных на контроль качества производимой лекарственной продукции и недопущение фальсификации лекарств.

Современным методом контроля лекарств является информационная система мониторинга движения лекарственных препаратов (ИС МДЛП).

С 1 июля 2020 г. данная информационная система успешно действует на территории Российской Федерации под наименованием «Честный знак». Информационное сопровождение происходит с использованием сайта https://xn--80ajghhoc2aj1c8b.xn--p1ai/, который также можно отыскать, введя в поисковой строке «честныйзнак.рф».

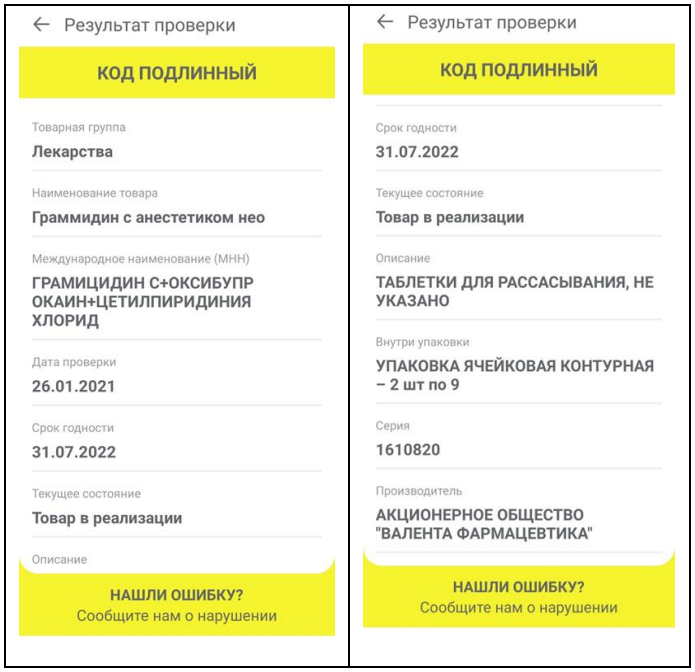
[1] URL: https://cutt.ly/Ekr9wTs (дата обращения: 26.01.2021).

Проверку подлинности лекарств может провести каждый желающий, используя приложение «Честный знак» для смартфона.

Проверка происходит путем считывания специального кода Data Matrix с вторичной (потребительской) упаковки лекарства. При этом все лекарства, произведенные после 1 июля 2020 г., должны иметь код Data Matrix.

Таким образом выглядит код Data Matrix, его можно сканировать прямо из этой статьи.

Результаты проверки выглядят следующим образом.



При проверке лекарства видны такие важные позиции как наименование, срок годности, текущее состояние – товар в реализации, серия и производитель.

На первый взгляд данная система выглядит волшебной, многообещающей, дает надежду полной защиты от фальсификации лекарств. Но при более детальном подходе видно, что указанный код Data Matrix с легкостью копируется и переносится на другие (поддельные) упаковки.

Наглядным образом это можно проверить путем считывания кода из данной статьи. Приложение покажет, что код считан с оригинальной упаковки, хотя статья не является упаковкой лекарства.

В условиях пандемии, недостатка лекарств и высокого спроса на них таким образом можно реализовать более 1000 пачек, выдавая их за одну партию. К примеру, препарат «арепливир» можно приобрести в аптеках за 12 320 руб.[1] Реализовав 1000 пачек фальсифицированного лекарства, злоумышленники заработают более 12 млн руб. Разобраться, каким образом разместить на упаковке код Data Matrix и изготовить аналогичную пачку, несложно и покажется многим интересным ради такой суммы.

Самое страшное, что при проверке кода Data Matrix на упаковке приложение покажет, что лекарственный препарат подлинный. О том, что его не стоит покупать, приложение покажет только после того, как партию снимут с продажи.

С учетом того, что препараты действуют на всех поразному, многие потребители даже не поймут, что принимали фальсификат. Качество печати позволяет воспроизводить упаковки в точном соответствии. О том, что упаковка фальсификата отличается от оригинальной, определят не сразу даже контролирующие органы.

Таким образом, ожидать от применения данной маркировки каких-то значимых достижений в борьбе с фальсификацией лекарств не приходится. Введение рассмотренной технологии усложняет жизнь лицам, занимающимся фальсификацией лекарств, однако полностью искоренить это явление не сможет.

В то же время указанная маркировка приносит свои результаты, поскольку эффективно препятствует появлению в лечебных учреждениях лекарств с истекшим сроком годности. Во-первых, реализация немаркированных лекарств после 1 июля 2020 г. запрещена, следовательно, все лекарства, произведенные до этого и срок годности которых истек, должны быть утилизированы. Во-

[1] URL: https://cutt.ly/ekrCc9D (дата обращения: 26.01.2021).

вторых, маркировка позволяет быстро определить лекарства с истекшим сроком годности.

Стоит отметить, что маркировка наносится только на вторичную упаковку. Переложить лекарства из одной упаковки в другую не составит труда. Также маркировка не станет препятствием для людей, профессионально занимающихся фальсификацией лекарств, поскольку они смогут изготовить вторичную упаковку и вложить в нее лекарства с истекшим сроком годности

Таким образом, действенного контроля в данной области удастся добиться только путем маркировки первичной упаковки. Но и в этом случае гарантировать 100-процентную защиту невозможно, так как найдутся умельцы, способные копировать код и на первичную упаковку.

Надлежащим образом данная система сможет работать только в том случае, если маркировка будет персональной, т.е. для каждой упаковки в отдельности, и если при считывании кода будут отражаться такие сведения, как дата реализации конечному потребителю. Только тогда можно быть полностью уверенным в том, что лекарство изготовлено надлежащим производителем и именно оно поступило в аптеку.

Изначально система задумывалась именно таким образом. Однако на практике реализовать эту идею оказалось невозможным, поскольку формирование кода в таком случае должно происходить непосредственно перед его нанесением на упаковку. Кроме того, быстро напечатать упаковки большой партией не представится возможным, поскольку перед печатью каждой пачки необходимо менять код и, соответственно, настройки печати.

Другой формой цифрового контроля является контроль движения лекарственных средств.

После формирования партии и ее отгрузки дистрибьютору производитель обязан сформировать сведения о наименовании и количестве лекарственных препаратов и выгрузить данные сведения в базу данных. В свою очередь дистрибьютор должен отметить данные о получении указанных лекарственных препаратов. И только после проверки системой соответствия представленных данных дистрибьютор сможет реализовывать лекарственные препараты. Дальнейшая цепочка реализации через посредников строится таким же образом вплоть до конечной аптеки или медицинского учреждения.

При реализации лекарственного препарата конечному потребителю информация о его реализации заносится в базу данных. После выбытия (использование в больнице, выдача по рецепту, продажа покупателю) лекарственных препаратов сведения о них выбывают из системы.

Такой подход позволяет не только контролировать подлинность лекарств, но и обладать сведениями о количестве тех или иных лекарств в какой-либо области, размерах их продажи. Оборот незарегистрированных лекарственных препаратов в таком случае полностью уйдет в теневой рынок, поскольку аптеки не смогут реализовывать такие товары.

Вместе с тем в применении и этой системы возникают определенные сложности, связанные с тем, что производители, дистрибьюторы и аптеки не успевают вносить сведения об отгрузке и приеме лекарств.

В связи с этим постановлением Правительства Российской Федерации от 02.11.2020 № 1779 упрощен порядок работы с системой мониторинга движения лекарственных препаратов. Аптеки и медучреждения могут выводить лекарства из оборота через кассы и регистраторы выбытия сразу после уведомления системы о поступивших к ним препаратах. Ждать подтверждения от системы, что сведения о приемке успешно зарегистрированы, не нужно[1]. Такие послабления введены до 1 июля 2021 г. Однако перенос принудительного применения этой системы происходит уже не первый раз, и нет никаких гарантий, что с 1 июля 2021 г. эта система заработает в полную силу.

Кроме того, описанная система позволяет отслеживать только лекарственные препараты, не охватывая прочие лекарственные средства, а также медицинские изделия и биологически активные добавки.

Наиболее эффективным, на наш взгляд, является сочетание обоих методов, если при этом будут введены следующие меры:

1. Уникальная в рамках одной партии маркировка первичной упаковки. При этом не обязательно первичная упаковка должна быть промаркирована таким сложным способом, как нанесение кода Data Matrix, достаточно указания номера путем штампования.

---

[1] URL: https://xn--80ajghhoc2aj1c8b.xn--p1ai/info/news/pravitelstvo-uprostilo-sistemu-markirovki-lekarstv/ (дата обращения: 26.01.2021).

2. Контроль перемещения лекарственных средств должен включать в себя указание не только номера партии, но и конкретных уникальных номеров лекарства. Таким образом проверяющие органы смогут сравнить, какие лекарства поступили в аптечные пункты или больницы с документами на их отгрузку. И если лекарств окажется больше или меньше либо не будут совпадать номера упаковок, то выявление фальсифицированных лекарств станет значительно проще. Соответственно, интерес к торговле фальсификатом резко упадет.

3. Продавцам лекарственных средств необходимо вести учет поступивших и проданных лекарств по уникальным номерам. Только в таком случае можно убедиться, что лекарств продано столько, сколько поступило от официальных производителей. Указание уникального номера в чеке позволит покупателю проверить добросовестность фармацевта.

В настоящее время национальной системой маркировки «Честный знак» в обязательном порядке маркируются такие товары, как шубы, табак, обувь, лекарственные препараты[1]. До конца 2020 г. введена обязательная маркировка фотоаппаратуры и шин.

Такой подход к выбору товаров представляется странным, поскольку приоритеты общественной значимости товаров, по нашему мнению, расставлены неверно. О том, когда планируется ввести обязательную маркировку медицинских изделий и биологически активных добавок, официальными источниками не сообщается.

Отсутствие обязательной маркировки на биологически активных добавках позволит недобросовестным продавцам реализовывать незарегистрированные лекарственные средства под видом БАДов.

В целях повышения качества работы системы по выявлению фальсифицированных лекарств предлагается разработать и внедрить техническую возможность индивидуальной маркировки каждой пачки лекарственных препаратов; среди сведений, доступных потребителю, отображать сведения о том, в какую конкретно аптеку или сеть поступила проверяемая пачка или партия лекарственных препаратов; в целях предотвращения реализации фальсифицированных, недобросовестных и незарегистрирован-

[1] URL: https://xn--80ajghhoc2aj1c8b.xn--p1ai/potrebitelyam/tovari-s-markirovkoj (дата обращения: 26.01.2021).

ных медицинских изделий и биологически активных добавок принять меры к обязательной их маркировке.

В целом Правительством Российской Федерации принимаются активные и действенные меры, направленные на борьбу с оборотом фальсифицированных лекарственных средств. Вместе с тем принятые меры являются недостаточными для эффективного предотвращения оборота фальсифицированных лекарственных средств. Соответственно, необходимо разрабатывать новые практические и теоретические методы и приемы борьбы с оборотом фальсифицированных и недобросовестных лекарственных средств и медицинских изделий.

А.С. Перина,
аспирант кафедры
уголовного права, криминологии
и уголовно-исполнительного права
Санкт-Петербургского юридического
института (филиала) Университета
прокуратуры Российской Федерации

Проблемы уголовно-правовой оценки преступлений, совершаемых в сети Darknet

Цифровизация и виртуализация общественной жизни отразились на современных тенденциях преступности, которые выходят за рамки мошеннических действий, совершаемых с использованием компьютерных технологий. Компьютерные технологии в настоящее время начали использоваться в качестве площадки для совершения преступлений, в том числе направленных против личности, здоровья населения.

Кроме того, интеллектуальное соперничество преступников и правоохранительных органов привело к усовершенствованию как методов противодействия преступности в этой сфере, так и способов совершения данных преступлений. Одним из последствий такого противостояния стал уход преступности в так называемый Darknet[1].

[1] *Мухин С.М.* Преступления в сети Darknet: краткая характеристика, проблем противодействия // Альманах молодого ученого. 2018. № 5.

В научной среде возникает необходимость глубокого и качественного изучения преступности в сфере высоких технологий, включая отдельные наиболее распространенные ее виды, комплексного анализа судебной практики, подготовки предложений по приведению законодательства в рассматриваемой сфере в соответствие с актуальными угрозами в первую очередь личности, но вместе с тем обществу и государству. Решения требуют проблемы, связанные с привлечением к ответственности администраторов крупных торговых площадок в сети Darknet, предоставляющих возможность и создающих условия для совершения в реальности таких преступлений против личности, как убийство, похищение человека, нарушение неприкосновенности частной жизни, доведение до самоубийства, оскорбление, вовлечение несовершеннолетних в совершение преступлений и пр. При этом обнаруживается общая тенденция увеличения использования компьютерных технологий в целом как площадки для достижения таких целей.

О сети Darknet как площадке, предоставляющей огромные возможности для нелегальных торговцев информацией, услугами и товарами, можно говорить с момента появления криптовалюты.

Термин «Darknet» (Даркнет), или «Тёмная паутина», в общем понимании обозначает совокупность веб-сайтов, видимых публично, но при этом имеющих скрытый IP-адрес сервера, на котором они размещаются. Такие сайты общедоступны для всех веб-пользователей, однако выяснить, кто является их автором, очень сложно. Также стоит сказать, что на подобные сайты невозможно попасть, используя популярные поисковые системы.

Даркнет – это частная сеть, в которой соединения устанавливаются только между доверенными пирами, иногда именующимися как «друзья», и чаще всего с использованием нестандартных протоколов и портов[1].

Безнаказанность противоправных действий такого рода дает повод ввести на законодательном уровне запрет анонимайзеров в сети, тем более что в некоторых странах (например, в Республике Беларусь[2]) подобная практика существует.

---

[1] *DarkNet:* темная сторона сети. URL: https://ipiskunov.blogspot.com/2016/08/darknet.html?m=1 (дата обращения: 24.01.2021).

[2] Постановление оперативно-аналитического центра при Президенте Республики Беларусь и Министерства связи и информатизации Республики Беларусь от 19.02.2015

Постановление Правительства Российской Федерации от 27.10.2018 № 1279 «Об утверждении Правил идентификации пользователей информационно-телекоммуникационной сети «Интернет» организатором сервиса обмена мгновенными сообщениями» устанавливает аналогичные запреты.

Однако разработка и совершенствование средств и методов противодействия преступности в сфере информационных технологий в таком ключе может ущемлять права законопослушных граждан, не имеющих целью использовать Даркнет как возможность совершения преступлений. Недопустимость указанного содержится в резолюции Совета по правам человека ООН от 22.05.2015, согласно которой анонимное использование сети «Интернет» и шифрование средств коммуникации признано неотъемлемым правом человека, гарантирующим его свободу слова и выражения мнения[1].

Вместе с тем специфика «новых» преступлений заключается в том, что их общественная опасность стала выходить за пределы одного государства и по своей функциональной направленности имеет международный характер[2]. Одной из причин криминализации Даркнета стала активная борьба правоохранительных органов с наркоманией. Затем Даркнет стал сетью для торговцев оружием, фальшивомонетчиков, сбытчиков поддельных документов, детской порнографии и пр.

Россия занимает первое место в мире по числу пользователей теневого Интернета 2019 г. Ежедневно в анонимную сеть выходят около 600 тыс. россиян[3].

В Даркнете существуют также объявления о таких услугах, как поджог машин, ограбления и избиения, фальсификация уголовных дел. Кроме того, Даркнет используется для совершения

№ 6/8 «Об утверждении Положения о порядке ограничения доступа к информационным ресурсам (их составным частям), размещенным в глобальной компьютерной сети Интернет». URL: https://pravo.by/document/?guid=12551&p0=T21503059&p1=1 (дата обращения: 22.01.2021).

[1] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, 22.05.2015. URL: https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc (дата обращения: 22.01.2021).

[2] *Мазур А.А.* Актуальные проблемы предупреждения преступности в социальной сети Даркнет // Вестн. Рос. ун-та кооперации. 2018. № 3(33). С. 126.

[3] *Россия* бьет рекорд за рекордом в даркнете. Что происходит? URL: https://www.bbc.com/russian/news-49007476 (дата обращения: 22.01.2021).

противоправных деяний, предусмотренных УК РФ (например, объявления о секс-услугах, распространение детской порнографии, распространение информации, защищенной авторским правом, преступления в сфере компьютерной информации)[1].

В настоящее время распространяется информация о наличии в Даркнете «красных комнат», под которыми предполагают закрытый сайт, где пользователи за определенную плату могут не только наблюдать за издевательствами, пытками, изнасилованиями и убийствами в режиме реального времени, но и принимать непосредственное участие в процессе, отдавая исполнителям команды через чат. Зарегистрированные пользователи Даркнета могут при этом сами оставить заказ об исполнении тех или иных преступных действий в их интересах[2].

Таким образом, анонимность лиц, которые совершают незаконные сделки в сети Даркнет, возможность совершать преступления, находясь в другой стране, «скрываться» за IP-адресом другого лица (как в деле Богатова[3]), анонимность лиц, заказывающих совершение преступлений, а также выполняющих заказы, создают сложности для уголовно-правовой оценки субъекта преступления, соучастников преступлений, количества эпизодов преступления, совокупности составов преступления, совершения нескольких преступлений одним и тем же лицом и т.д. Кроме того, сложности возникают и при установлении ответственности лиц, которые предоставляют площадку для совершения уголовно наказуемых деяний.

Ответственность таких лиц должна быть реализована в уголовном праве ввиду повышенной общественной опасности их действий. Анализ способов международной борьбы с преступностью в сети Даркнет, предупредительной работы позволит выработать основные уголовно-правовые методы борьбы с преступлениями, совершаемыми в сети Даркнет, и внедрить в действующее уголовное законодательство Российской Федерации.

Принятие комплексных мер по противодействию данному виду преступности, включающих как современные информационно-технические методы борьбы, так и своевременное совер-

---

[1] *Мазур А.А.* Указ. соч.

[2] Там же.

[3] *Дело* Богатова: как повесить статью о терроризме на один IP-адрес. URL: https://www.bbc.com/russian/features-39590931 (дата обращения: 22.01.2021).

шенствование уголовного законодательства, позволяющее персонализировать ответственность лиц, предоставляющих площадку, информационные ресурсы и технологии для совершения преступлений в сети «Интернет» в условиях анонимности, необходимо на государственном уровне.

А.Г. Себякин,
руководитель второго экспертного отдела (с дислокацией в г. Иркутске) Сибирского филиала Судебно-экспертного центра Следственного комитета Российской Федерации

Принципы изъятия и криминалистического исследования информационных носителей

Продолжающаяся цифровизация человеческой деятельности не только поддерживает, но и неизбежно повышает интерес ученых к различным аспектам исследования компьютерных систем с целью получения криминалистически значимой информации. В настоящее время научная активность в указанной сфере настолько высока, что обсуждение проблем, прямо или косвенно касающихся тематики электронно-цифровых следов, перешло из формата отдельных публикаций в формат регулярных научно-практических конференций[1] и тематических выпусков научных журналов[2].

Решение значительной части рассматриваемых вопросов зависит от общих правил или принципов криминалистического исследования цифровых носителей информации, на которые оно опирается. Однако в динамично меняющейся цифровой реальности указанные принципы также не являются фундаментально неизменными. Сегодня в качестве базовых принципов криминалистического исследования информационных носителей традиционно принимаются постулаты, выделенные Е.Р. Россинской:

---

[1] *Цифровой* след как объект судебной экспертизы: материалы Междунар. науч.-практ. конф. М.: Проспект, 2020.

[2] *Развитие* теории и совершенствование практики использования специальных знаний в условиях цифровизации // Вестн. криминалистики. 2020. № 2 (74).

1. Не должна изменяться никакая информация, содержащаяся на изымаемых носителях компьютерной информации (принцип неизменности информации).

2. Доступ к информации и исследование ее на месте допустимы, только когда невозможно изъять носитель для производства судебной экспертизы (принцип обязательного изъятия носителя).

3. Любые манипуляции с компьютерными средствами и системами должны осуществляться только с участием специалиста (принцип обязательного участия специалиста).

4. Все выполняемые действия должны подробно протоколироваться, чтобы обеспечить возможность использования результатов этих действий в доказывании (принцип протоколирования действий)[1].

Из всех перечисленных принципов безусловным является принцип обязательной процессуальной фиксации, поскольку доказательства в уголовном судопроизводстве получают только в установленном законом порядке.

Принцип неизменности информации обладает огромной важностью, но необходимо учитывать, что информация на цифровом носителе может храниться на различных участках и характер этой информации также может быть различен. Необходимо в максимальной степени придерживаться данного принципа, однако он практически не может быть соблюден, например, при исследовании памяти мобильных устройств, имеющих парольную защиту и шифрование данных. Стандартные методы извлечения пользовательских данных из раздела *User Data* в подобных случаях сопряжены с неизбежной подменой загрузчика, т.е. изменением информации в разделе *boot* (для операционных систем Android). Указанный алгоритм используют в своих аппаратно-программных комплексах UFED и «Мобильный криминалист» ведущие компании в области криминалистического исследования мобильных устройств Cellebrite и Oxygen Software. Тем не менее операции с разделом *boot* не вносят изменений в раздел *User Data,* и по отношению к указанному разделу принцип неизменности информации считается соблюденным. То же касается и из-

[1] *Россинская Е.Р.* К вопросу о частной теории информационно-компьютерного обеспечения криминалистической деятельности // Изв. Тул. гос. ун-та. Эконом. и юрид. науки. 2016. № 3–2. С. 115.

влечения информации с систем видеорегистрации, использующих проприетарные файловые системы: в основной массе подобных случаев информация извлекается с применением штатных средств выгрузки системы видеорегистрации путем ее активации (включения), что ведет к изменению служебной информации.

Еще более неоднозначным является принцип обязательного изъятия носителя, поскольку доступ к информации и исследование ее на месте зачастую являются единственно возможным способом закрепления фактов. Например, при наличии установленного авторизованного VPN-соединения (в частности, при незаконных организации и проведении азартных игр) существует возможность изъятия носителя, но информативность электронно-цифровых следов, оставшихся на нем после изъятия, будет существенно ниже, чем в случае, если фиксацию данных следов осуществить на месте, т.е. без изъятия носителя: изъятие носителя сопровождается разрывом сетевого соединения, восстановление которого при отсутствии сведений об учетной записи не представляется возможным. Таким образом, сведения, которые могли бы быть получены при наличии сетевого подключения, становятся недоступными. В научной литературе уже высказывались суждения о возможности дистанционного исследования «с трансляцией необходимой информации по каналам связи без необходимости физического перемещения носителя информации»[1]. Ввиду изложенного соблюдение второго принципа не всегда эффективно с точки зрения доказывания. По нашему мнению, вопрос изъятия носителя должен решаться совместно со специалистом в области компьютерной техники, который способен оценить степень риска утраты электронно-цифровых следов. В данном контексте приоритетным способом изъятия информации будет ее копирование, а не изъятие носителя[2].

Обсуждаемый принцип предлагается именовать принципом *мотивированного изъятия носителя*. Смысл принципа заключается в том, что изъятие носителя производится только при наличии объективных причин полагать, что на нем может содержать-

---

[1] *Степаненко Д.А.* Криминалистическая наука в реалиях информационного общества // материалы Междунар. науч.-практ. конф. «Криминалистические чтения на Байкале – 2015». Иркутск: РГУП, Восточно-Сибир. филиал, 2015. С.109.

[2] *Гаврилин Ю.В., Победкин А.В.* Собирание доказательств в виде сведений на электронных носителях в уголовном судопроизводстве России: необходимо совершенствование процессуальной формы // Тр. Акад. управления МВД России. 2018. № 3 (47). С. 110.

ся информация, которую невозможно обнаружить на месте. Возможность доступа к информации и ее исследования без изъятия носителя определяется следственной ситуацией и решаемой тактической задачей.

Спорным выглядит и третий принцип (обязательного участия специалиста). В настоящее время указанный принцип в отношении изъятия электронных носителей закреплен в ч. 2 ст. 164[1] УПК РФ: «Электронные носители информации изымаются в ходе производства следственных действий с участием специалиста». В свете неизменного технологического тренда на увеличение количества и разнообразия электронных носителей практическая реализация данного принципа труднодостижима. Вопрос целесообразности обязательного участия специалиста при изъятии электронного носителя уже обсуждался в научной литературе[1]. Изъятие электронных носителей, являющихся автономными устройствами (мобильный телефон, оптический диск, портативный жесткий диск, флеш-накопитель и пр.), не требует манипуляций с привлечением специальных знаний. Такие носители могут быть изъяты непосредственно следователем без нарушения целостности хранящейся на них информации. В подобном случае мы разделяем мнение Ю.В. Гаврилина о том, что требование нормы УПК РФ об обязательном участии специалиста при проведении обыска или выемки, в ходе которых осуществляется изъятие электронных носителей информации, «выглядит чрезмерным и неоправданным»[2].

А.В. Закомолдиным высказана идея о необходимости законодательного закрепления понятия «электронный носитель информации», а также определения случаев необязательного участия специалиста при изъятии электронного носителя информации[3]. Мы солидарны с приведенным мнением при условии дифференцирования электронных носителей по критерию возможности их изъятия без применения специальных знаний.

С данной задачей соотносится вопрос дифференциации знаний в области компьютерной техники на специальные и про-

---

[1] *Зуев С.В.* Развитие информационных технологий в уголовном судопроизводстве: монография М.: Юрлитинформ, 2018. С. 35–36.

[2] *Гаврилин Ю.В.* Электронные носители информации в уголовном судопроизводстве // Тр. Акад. управления МВД России. 2017. № 4 (44). С. 46.

[3] *Закомолдин А.В.* Проблемы определения критерия необходимости в привлечении специалиста при изъятии электронных носителей информации в уголовном процессе России // Вектор науки ТГУ. Сер.: Юрид. науки. 2019. № 1 (36). С.11.

фессиональные. Специальные знания традиционно связаны с фигурами эксперта и специалиста (ст. 57 и 58 УПК РФ соответственно). Именно поэтому подход с обязательным участием специалиста является несколько суженным, так как подразумевает применение только специальных знаний. Под профессиональными же знаниями подразумевается совокупность теоретических научных сведений и познаний, а также осведомленность в определенной сфере деятельности, необходимые для качественного исполнения должностных обязанностей с целью достижения результатов в профессиональной служебной деятельности[1]. В соответствии с профессиональным стандартом «Следователь-криминалист» [2] часть операций с цифровыми носителями информации может быть выполнена следователем-криминалистом в рамках применения своих профессиональных знаний без привлечения специалиста.

Таким образом, принцип обязательного участия специалиста можно трансформировать в *принцип обязательного участия компетентного лица* (т.е. лица, обладающего специальными или профессиональными знаниями в области компьютерной техники). Термин «компетентное лицо» не имеет процессуальной окраски и регламентирует лишь наличие определенного уровня знаний (компетентности) в области компьютерной техники. Тип этих знаний (профессиональные, специальные), а также форма их применения должны зависеть от вида информационного носителя и определяться тактической задачей, стоящей перед следователем.

Обобщая изложенное, можно сделать вывод, что принципы криминалистического исследования информационных носителей в силу динамичного развития компьютерной техники также не являются статичными. Толкование принципов в предложенной редакции позволит следователю реализовать более гибкий механизм разрешения задач расследования и будет способствовать рациональному использованию материальных и трудовых ресурсов как организационной составляющей планирования тактических действий.

---

[1] Приказ Ростехрегулирования от 30.08.2007 № 2358 «Об организации работы по проведению конкурсов на замещение вакантных должностей федеральной государственной гражданской службы Российской Федерации в Федеральном агентстве по техническому регулированию и метрологии».

[2] Приказ Минтруда России от 23.03.2015 № 183н «Об утверждении профессионального стандарта «Следователь-криминалист».

А.А. Федосеева,
аспирант кафедры
уголовно-процессуального права
и криминалистики Всероссийского
государственного университета юстиции
(РПА Минюста России)

Об актуальных проблемах организационного обеспечения раскрытия и расследования преступлений против конституционного права человека на неприкосновенность частной жизни, совершенных с использованием информационно-коммуникационных технологий

Повсеместное внедрение информационно-коммуникационных технологий и их разнообразие, цифровизация всех сфер жизнедеятельности человека являются детерминирующим фактором в качественном изменении структуры преступной деятельности: субъекты преступной деятельности получили безграничные возможности и способы подготовки, совершения и сокрытия своих неправомерных действий. Сегодня проблема борьбы с преступлениями, совершенными с применением информационных технологий, приобрела глобальный характер, являясь актуальной для большинства стран.

Согласно статистическим данным ГИАЦ МВД России за январь – ноябрь 2020 г., правоохранительными органами зарегистрировано более 461 тыс. преступлений, совершенных с использованием информационно-коммуникационных технологий или в сфере компьютерной информации (рост по сравнению с аналогичным периодом 2019 г. составил 76,6%, в 2018 г. – 195,07%[1]). Безусловно, в структуре IT-преступлений доминируют кражи, мошенничество, незаконный сбыт наркотических средств или их аналогов. Однако исходя из данных формы № 4-ЕГС[2] преступления, предусмотренные ст. 137 и 138 УК РФ, также совершаются с использованием названных технологий (количество зарегистри-

[1] Краткая характеристика состояния преступности в Российской Федерации. URL: https://мвд.рф (дата обращения: 11.01.2021).
[2] Генеральная прокуратура Российской Федерации. Портал правовой статистики. URL: http://crimestat.ru/analytics (дата обращения: 11.01.2021).

рованных преступлений за январь – ноябрь 2020 г. составляет 898, за аналогичный период 2019 г. – 639).

Преступления против конституционного права человека на неприкосновенность частной жизни обладают рядом особенностей, влияющих на степень их общественной опасности, а также тактику и методику их расследования. Данные преступления носят чаще всего дистанционный характер, характеризуются усложненным способом их подготовки (например, использование программного обеспечения, посредством которого может быть изменен IP-адрес устройства, с которого осуществлялся доступ в сеть «Интернет» (VPN, TOR, SSL и др.); технологий, позволяющих осуществлять подмену абонентских номеров – SIP-телефония, что позволяет решить как минимум две задачи, стоящие перед преступниками: увеличение степени анонимности и облегчение сокрытия следов преступления). Для получения личных данных потерпевшего могут быть использованы методы и методики социальной инженерии, психологического воздействия и НЛП (фактически лицо на добровольной основе предоставляет преступнику свои личные данные). Кроме того, нежелание потерпевших контактировать с представителями правоохранительных органов в силу стыда, правового нигилизма, внушаемости (колоссальным образом возрастает степень латентности данного вида преступлений) и т.д. Важнейшей особенностью данного вида преступлений являются механизм следообразования, сами следы (информационные или цифровые) и их локализация (путь прохождения информационного сигнала), что вызывает ряд сложностей при работе с ними и необходимость специализированной подготовки субъектов расследования преступлений.

Изложенное обусловливает необходимость повышения эффективности борьбы с преступлениями против конституционного права на неприкосновенность частной жизни, совершенными с использованием информационно-коммуникационных технологий. В данном случае проблему представляется возможным решить, используя разработки криминалистического обеспечения, под которым профессор А.Ф. Волынский предлагает понимать систему действий, направленных на формирование условий постоянной готовности правоохранительных органов к применению криминалистических методов в раскрытии и расследовании пре-

ступлений[1]. Криминалистическое обеспечение – это сложное и многоаспектное явление, главным структурным элементом которого выступает правовое обеспечение. В свою очередь центральным элементом в механизме реализации правовых предписаний является организационное обеспечение, т.е. «система взаимосвязанных элементов технико-криминалистического, тактико-криминалистического, научно-методического, организационно-кадрового и правового характера, направленная на создание условий постоянной готовности и практической реализации правоохранительными органами в раскрытии и расследовании преступлений, в конкретно определенный период времени»[2].

Если рассматривать преступления, предусмотренные ст. 137 и 138 УК РФ (учитывая характер и способ их совершения), как составляющую большого пласта преступлений, совершенных с применением информационных и телекоммуникационных сетей, то представляется возможным говорить о наличии ряда проблем у лиц, осуществляющих предварительное расследование, в получении криминалистически значимой информации электронного вида от интернет-провайдеров, хостинг-провайдеров, операторов, предоставляющих услуги связи, интернет-сервисов, социальных сетей и мессенджеров. Решить данную проблему можно путем внедрения электронного документооборота на основании двустороннего соглашения между правоохранительными органами и названными субъектами, следовательно, правоохранительные органы получат практически мгновенный доступ к криминалистически значимой информации для расследования уголовных дел и установления виновных лиц.

Также существует проблема в области криминалистического учета и идентификации электронно-цифровых следов гаджетов. Современные базы данных не отвечают требованиям: отсутствие колоссальных вычислительных мощностей; недостаточный штат сотрудников, которые могут обеспечить постоянную работу этих устройств; машины собирают информацию, не отвечающую целям расследования преступлений данного вида: сведения, позво-

---

[1] *Волынский А.Ф.* Криминалистическое обеспечение раскрытия и расследования преступлений: учеб. пособие. М.: Моск. ун-т МВД России им. В. Я. Кикотя, 2016. С. 43.

[2] *Першин А.Н., Белов И.Т.* Содержание криминалистического обеспечения расследования преступлений // Ученые-криминалисты и их роль в совершенствовании научных основ уголовного судопроизводства (ч. 2): сб. науч. тр. М.: Акад. МВД России, 2007. С. 275.

ляют идентифицировать лишь персональные данные пользователя, а не данные, указывающие на устройство, используемое злоумышленником. Эту проблему пытаются решить на базе ФСБ России[1].

Проблему, касающуюся нехватки кадров, обладающих достаточными знаниями и навыками, которые позволят поддерживать работу «вычислительных машин» и осуществлять постоянную их модификацию (создание новых алгоритмов работы), представляется возможным решить путем внедрения специальных учебных курсов, профильных дисциплин в высших учебных заведениях, где осуществляется профильная подготовка специалистов для правоохранительных органов и экспертно-криминалистических подразделений[2].

В заключение хотелось бы отметить, что на криминалистику, в частности на криминалистическое обеспечение, возложена колоссальная нагрузка, она несет в себе социальную функцию[3], решается ряд сложных и принципиально значимых задач, основной из которых является формирование положительного общественного мнения о деятельности правоохранительных органов, увеличение уверенности населения в том, что лица, осуществляющие расследование IT-преступлений (вне зависимости от того, в какой сфере они совершены), обладают всем спектром возможностей для разрешения уголовного дела: восстановление прав потерпевшего, неотвратимость наказания виновных лиц, восстановление социальной справедливости.

---

[1] Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации утв. Президентом РФ 12.12.2014 № К 1274.

[2] Так, на базе Московского университета МВД России им. В.Я. Кикотя совместно со Следственным департаментом МВД России, экспертно-криминалистическим центром МВД России, Банком России, ПАО «Сбербанк» и АО «Лаборатория Касперского» была создана программа повышения квалификации следователей «Совершенствование деятельности подразделений предварительного следствия органов внутренних дел по расследованию преступлений в сфере компьютерной информации, совершаемых против собственности». URL: https://мосу.мвд.рф (дата обращения:10.01.2021).

[3] *Волынский А.Ф.* Криминалистическое обеспечение раскрытия и расследования преступлений как форма реализации социальных функций криминалистики // Юрид. наука и правоохран. практика. 2008. № 3 (6).

В.К. Барчуков,
соискатель Высшей школы
государственного аудита
Московского государственного
университета имени М.В. Ломоносова

Применение элементов искусственного интеллекта в деятельности прокуратуры: современное состояние и перспективы

После того как Дж. Маккарти на Дартмутской конференции в 1956 г. впервые употребил термин «искусственный интеллект», эта идея прочно укоренилась в сознании миллионов и используется специалистами, в том числе и в правоохранительной деятельности.

Наряду с термином «искусственный интеллект» в научной и специальной литературе выделяют ряд смежных понятий. Так, в частности, говоря об искусственном интеллекте, чаще всего его отождествляют с такими понятиями, как «робот», «искусственная интеллектуальная система», «искусственная интеллектуальная технология», «нейронная сеть», «машинное обучение» и др. А в отдельных случаях упрощенно представляют как обычную компьютерную программу, что не соответствует действительности. По нашему мнению, если искусственный интеллект – это комплекс программно-аппаратных средств, отличительной особенностью которых является способность заменить когнитивные функции человека, то нейронные сети – это набор технологических решений, интеллектуальных средств, позволяющих достичь задач, стоящих перед искусственным интеллектом, глубинное обучение и машинное обучение – это комплекс технологических решений, позволяющих определенным образом организовать нейронные сети, чтобы они эти задачи выполняли, т.е. являются элементами искусственного интеллекта. Робот – это автономная совокупность программно-технических устройств, искусственная интеллектуальная система – система, включающая в себя как технологии искусственного интеллекта, так и иные технологические решения. Искусственную интеллектуальную технологию можно определить как систему способов и средств, реализованных в программно-аппаратных комплексах, обеспечивающих

функционирование информационного цикла (полностью или частично), направленных на решение задач, стоящих перед человеком, принимающих решения автономно или с помощью человека.

Согласно проведенному исследованию применение искусственного интеллекта в ПО, в частности в органах прокуратуры, возможно исключительно под контролем человека. В противном случае обезличенный правоприменительный процесс может привести к неконтролируемым последствиям, связанным как с нарушением прав и законных интересов граждан, так и с искажением сути российского судопроизводства и правосудия. Более того, на текущем этапе развития информационного общества возможно применение лишь некоторых элементов искусственного интеллекта.

Концепция цифровой трансформации органов и организаций прокуратуры предусматривает внедрение информационно-аналитической обработки данных с использованием технологий искусственного интеллекта и больших данных до 2020 г. Однако опрос работников прокуратуры показал, что до сих пор указанные системы находятся на стадии разработки.

Так, нерешенными в настоящие время остаются вопросы, связанные с принятием решений, имеющих определенный правовой статус, оформлением данных решений в виде документов, придающих им необходимый правовой статус и обеспечивающих практическую реализацию правовых последствий. То есть речь идет не только о практическом осуществлении прокуратурой функций, которые возложены на нее государством, но и о надлежащем отражении данной деятельности в соответствующей документации.

Так, при ручной обработке контроль за сохранением правового статуса обеспечивается сотрудниками в рамках их должностных полномочий. Если же обработка осуществляется в автоматизированном режиме, то неизбежно встает вопрос о том, возможно ли обеспечить аналогичные ручным технологии контроля.

Поскольку основные акценты делаются не на решение технических проблем, а на вопросы правового характера, большое внимание уделяется особенностям применения таких информационных технологий, нацеленных на уточнение характера диссипации правового статуса.

Прежде всего, для этого исследовались различные виды документов, характерных для деятельности прокуратуры, включая входящие, внутренние и исходящие документы.

В частности, исследовались особенности обработки таких видов информации, которые перечислены в ч. 1 ст. 140 УПК РФ в качестве поводов для возбуждения уголовного дела, а затем детализированы в ст. 141–143 УПК РФ: заявление о преступлении в устной и письменной форме (ст. 141 УПК РФ), заявление о явке с повинной в устной и письменной форме (ст. 142 УПК РФ), рапорт об обнаружении признаков преступления (ст. 143 УПК РФ), сообщение о совершенном или готовящемся преступлении, полученное из иных источников (п. 3 ч. 1 ст. 140 УПК РФ), сообщение о преступлении, распространенное в средствах массовой информации, рассмотренное прокурором и направленное с поручением прокурора органу дознания или по поручению руководителя следственного органа следователю (п. 4 ч. 1 ст. 140, ч. 2 ст. 144 УПК РФ). Важно обратить внимание на процедуры, которые определяют переход определенной информации в новый правовой статус.

В системе органов прокуратуры определены некоторые процедуры придания правового статуса информации. Вместе с тем выделяется ряд проблем, связанных с контролем за сохранением правового статуса электронных документов.

В первую очередь были рассмотрены особенности применения компьютерных роботов, функционирующих на основе нейросетевых алгоритмов. Особенность данного элемента связана с его настройкой или «обучением» путем адаптации к специально отобранной совокупности аналогичных ситуаций. Использование прецедентов характерно для англосаксонской правовой семьи. Поскольку российская правовая система основана на принципах, тяготеющих к семье континентального права, применение данных видов искусственного интеллекта создает высокие риски потери правового статуса результатов обработки информации, используемой в деятельности правоохранительных органов.

В то же время применение нейросетевых алгоритмов открывает ряд принципиально новых возможностей в рамках интерактивных экспертных систем. Речь идет о формировании нескольких этапов применения элементов искусственного интеллекта в рамках организации диалога с участием оператора, позволяющей

контролировать изменение правового статуса промежуточных и итоговых результатов обработки.

Еще одним элементом искусственного интеллекта являются гипертекстовые технологии, имеющие большой потенциал. Но для его раскрытия необходимо формализовать ряд давно назревших проблем, на которые неоднократно обращали внимание ученые.

Прежде всего, речь идет об особенностях изложения правовых предписаний, которые применяются в процессе законотворчества, а затем создают серьезные проблемы при правоприменении. В частности, особенности уголовно-правовой характеристики преступлений с учетом явно выраженного бланкетного характера многих диспозиций, раскрытие которых требует применения других уголовно-правовых и гражданско-правовых норм. В связи с этим Л.Д. Гаухман отмечал, что от правоприменителя требуется, чтобы он знал все законы и иные нормативные правовые акты, на которые де-факто сделаны ссылки в бланкетных диспозициях Особенной части УК РФ, а также помнил, в какой момент или до какого периода они действуют в той или иной редакции, и имел реальную возможность их найти[1].

Во многих случаях это создает настолько серьезные проблемы у правоприменителей, что некоторые нормы из-за субъективного подхода к их раскрытию применяются редко. Именно к таким видам преступлений относится существенная часть уголовных дел, которые буквально разваливаются в суде.

Решение части этих проблем возможно на основе применения гипертекстовых технологий, опирающихся на специально созданную систему тезаурусов – профессионально составленных и научно обоснованных определений наиболее часто используемых в диспозициях уголовно-правовых норм понятий и всего многообразия связей между ними. Их принципиальное отличие от живого, развивающегося русского языка в том, что тезаурусы опираются на такие языковые системы, которые принято называть мертвыми, поскольку используемая в них система понятий и связей между ними зафиксирована на определенный момент и добавление новых понятий в них запрещается. По мере развития нормативно-правовой базы, в которой используются новые поня-

[1] *Гаухман Л.Д.* Нужна правовая экспертиза по уголовным делам // Законность. 2000. № 4.

тия, создается новый тезаурус, уже фиксирующий используемую систему понятий на другой момент времени.

Первый тезаурус может быть сориентирован на раскрытие содержательных особенностей той части бланкетных диспозиций уголовно-правовых норм, которая связана с применением других уголовно-правовых норм как Общей части, так и Особенной части Уголовного кодекса Российской Федерации. По сути, основная цель создания тезауруса заключается в разъяснении критериев, которые могут применяться для разграничения различных видов преступлений со схожими признаками.

Другие тезаурусы связаны с применением для раскрытия бланкетных диспозиций данных уголовно-правовых норм положений гражданского и специального законодательства.

Формализации такого рода разъяснений в рамках современных гипертекстовых технологий позволят не только доходчиво донести до участников уголовного судопроизводства все особенности развернутой уголовно-правовой характеристики определенного преступления, но и обеспечить необходимый правовой статус такого рода разъяснений.

Кардинальным выходом в данной ситуации представляется создание единого юридического алгоритмического языка, универсального для деятельности всех правоохранительных органов.

Рекомендации

I Всероссийской научно-практической конференции
«Цифровые технологии в борьбе с преступностью: проблемы, состояние, тенденции (Долговские чтения)»

27 января 2021 г. г. Москва

Участники Всероссийской научно-практической конференции – научные, педагогические и практические работники Генеральной прокуратуры Российской Федерации, Университета прокуратуры Российской Федерации, Антитеррористического центра государств – участников СНГ, Научно-практического центра проблем укрепления законности и правопорядка Генеральной прокуратуры Республики Беларусь, Московской академии Следственного комитета Российской Федерации, ВНИИ МВД России, Московского университета МВД России имени В.Я. Кикотя, Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации, иных научных, образовательных и общественных организаций, обсудив актуальные проблемы использования информационных технологий в борьбе с преступностью, современное состояние и тенденции преступности в сфере информационно-коммуникационных технологий и компьютерной информации, вопросы специфики международного сотрудничества и совершенствования мер противодействия киберпреступности, **отмечают** следующее.

Цифровизация и виртуализация общественной жизни не только отразились на современных тенденциях преступности, но и актуализировали вопросы использования информационных технологий при противодействии этому негативному социальному явлению. Причем существующие научные разработки давно вышли за рамки обеспечения расследования преступлений в сфере компьютерной информации. Активно разрабатываются методики сбора и исследования цифровой информации, сохраненной в различных информационных объектах.

На информационную составляющую обращается внимание в организационно-распорядительных документах Генерального прокурора Российской Федерации, что закономерно связано с

необходимостью внедрения и использования современных и перспективных цифровых технологий обработки первичной информации во всех видах надзорной деятельности в целях повышения оперативности прокурорского реагирования.

Возможности инновационных технологий непосредственно используются в деятельности по предупреждению, раскрытию и расследованию преступлений. В правоохранительных органах создаются специализированные экспертные подразделения, вводятся в эксплуатацию базы данных (регистрационные, справочно-информационные и аналитические системы). На фоне роста числа киберпреступлений во время пандемии COVID-19 поставлен вопрос о создании киберполиции в структуре органов МВД России, функцией которой будет регистрация сообщений о нарушениях в сети «Интернет», в том числе в социальных сетях.

В рамках современной политики цифровизации происходит трансформация деятельности государственных контролирующих органов (Росфинмониторинга, Банка России, ФНС России), а также финансовых организаций. В то же время не все ведомства находятся на одном технологическом уровне развития, различия подходов и используемого инструментария нередко усложняют синхронизацию информации для обмена, использования цифровых документов и электронной цифровой подписи.

Одновременно с цифровизацией правоохранительной деятельности, ростом рынка телекоммуникаций и пользовательской базы возрастают и возможности эксплуатации сети «Интернет» в противоправных целях.

Одним из основных негативных факторов, влияющих на состояние информационной безопасности, является наращивание рядом зарубежных стран возможностей информационно-технического воздействия на информационную инфраструктуру в военных целях. Одновременно с этим усиливается деятельность организаций, осуществляющих техническую разведку в отношении российских государственных органов, научных организаций и предприятий оборонно-промышленного комплекса.

Расширяются масштабы использования специальными службами отдельных государств средств оказания информационно-психологического воздействия, направленного на дестабилизацию внутриполитической и социальной ситуации в различных

регионах мира и приводящего к подрыву суверенитета и нарушению территориальной целостности других государств. В эту деятельность вовлекаются религиозные, этнические, правозащитные и иные организации, а также отдельные группы граждан, при этом широко используются возможности информационных технологий.

Отмечается тенденция к увеличению в зарубежных средствах массовой информации так называемых фейков, касающихся нашей страны. Наращивается информационное воздействие на население России, в первую очередь на молодежь, в целях размывания традиционных российских духовно-нравственных ценностей, ее радикализации и вовлечения в протестную активность.

В последние годы наблюдается прогнозируемое увеличение количественных показателей киберпреступности. За три последних года количество преступлений, совершенных с использованием информационно-коммуникационных технологий и в сфере компьютерной информации, выросло втрое (с 174 674 в 2018 г. до 510 396 в 2020 г.). Возрос и удельный вес преступности данного вида в общем количестве зарегистрированных преступлений. Если в 2018 г. удельный вес не превышал 10% (174 674 из 1 991 532), то в 2020 г. доля киберпреступлений составила четверть всей преступности (510 396 из 2 044 221). Угрозой национальной безопасности является распространение экстремистской идеологии в информационных сетях, оказывающее влияние на динамику террористической и экстремистской преступности.

Резкое увеличение количества регистрируемых преступлений не всегда сопровождается принятием необходимых мер противодействия и предупреждения преступности данного вида. В этом отношении очевидна необходимость принятия мер, направленных на повышение квалификации сотрудников правоохранительных органов, более глубокое освоение современных криминалистических методик. Нуждается в совершенствовании техническая оснащенность правоохранительных, надзорных и контролирующих органов.

Одновременно с этим требуется противодействие нарушениям в сфере персональных данных. Факты неправомерного распространения личной информации встречаются в правоприменительной деятельности как органов государственной власти, так и

негосударственных структур, наделенных правом доступа к информации частного характера.

Достижение значимых результатов в борьбе с преступлениями в сфере информационно-телекоммуникационных сетей невозможно без формирования системы международной информационной безопасности. На этом направлении Российская Федерация предпринимает серьезные усилия. Так, в декабре 2019 г. Генеральная Ассамблея ООН в принятой на 74-й сессии резолюции выразила поддержку инициативы нашей страны о разработке международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях. Это своевременное решение ввиду отсутствия сегодня эффективных механизмов регулирования в сфере противодействия киберпреступности. В свою очередь, положения Конвенции Совета Европы о киберпреступности (Будапешт, 2001) – основного международно-правового акта в сфере противодействия преступности с использованием информационных технологий – в значительной мере устарели.

Формирование системы международно-правового регулирования противодействия киберпреступности предполагает наличие единообразного понятийного аппарата, используемого в текстах правовых документов.

Принимая во внимание данное обстоятельство, требуют унификации такие термины, как «компьютерный инцидент», «сайт в сети «Интернет», «поисковая система», «доступ к информации», «конфиденциальность информации», «сетевой адрес», «владелец сайта в сети «Интернет», «критическая информационная инфраструктура», «объекты критической инфраструктуры», «бот-сеть», «вредоносная программа», «детская порнография».

На основе результатов проведенных криминологических исследований и их обсуждения участники конференции **рекомендуют**:

1. Обратить особое внимание на совершенствование кадрового обеспечения деятельности правоохранительных органов в условиях адаптации к цифровой реальности. Прежде всего это касается профессиональной переподготовки, повышения квалификации и специализации сотрудников с учетом возможного перехода в перспективе к расширению перечня электронных про-

цессуальных документов и формированию электронных уголовных дел. В частности, своевременной корректировки и актуализации требуют образовательные программы высшего юридического образования и программы повышения квалификации сотрудников правоохранительных органов. Кроме того, насущной потребностью является модернизация прокурорского надзора.

2. В целях дальнейшего усиления межведомственного и межгосударственного взаимодействия представляется необходимым создание единых баз данных, позволяющих оперативно осуществлять обмен информацией о совершенных преступлениях. Кроме того, требуется принятие мер по совершенствованию методов противодействия преступности, включая закрепление в уголовно-процессуальном законодательстве требований к собиранию доказательств с использованием электронных технологий.

3. Необходимо глубокое и качественное изучение преступности в сфере высоких технологий, включая отдельные наиболее распространенные ее виды, проведение комплексного анализа следственной и судебной практики по киберпреступлениям. Особое внимание должно быть сосредоточено на проблемах привлечения к ответственности администраторов крупных торговых площадок в Даркнете, выявления и предупреждения преступлений, связанных с использованием цифровых валют, социальной инженерии, сексуальной эксплуатацией несовершеннолетних, незаконным оборотом наркотических средств в сети «Интернет» и распространением экстремистских материалов.

4. В целях обеспечения информационной безопасности Российской Федерации следует рассмотреть вопрос о закреплении правового статуса социальных интернет-сетей, уделив особое внимание идентификации их владельцев и закреплению обязанностей данных лиц:

по недопущению распространения и передачи информационных сообщений, используемых при осуществлении противоправной деятельности, а также обмена ими между пользователями;

по ограничению распространения пользователями сети «Интернет» общественно значимой достоверной информации о государственной политике Российской Федерации и ее официальной позиции по социально значимым событиям в стране и мире.

5. Формирование системы международно-правового регулирования противодействия информационной преступности предполагает наличие единообразного понятийного аппарата, используемого в текстах правовых документов. К одному из основных направлений государственной политики Российской Федерации в сфере международной информационной безопасности относится содействие созданию международного механизма постоянного контроля за недопущением использования информационных и коммуникационных технологий в террористических (экстремистских) целях, в том числе в целях вмешательства во внутренние дела суверенных государств.

6. Для преодоления новых внутренних вызовов и угроз, связанных с производством и оборотом цифровой валюты в Российской Федерации, представляется необходимым осуществить мониторинг применения Федерального закона от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации». В целях возможности ареста и конфискации цифровой валюты в гражданском, административном и уголовном судопроизводстве Российской Федерации предлагается отнести ее к объектам гражданских прав, в частности к категории имущества.

7. Предлагается законодательно закрепить механизм отнесения объектов информационной инфраструктуры к критически важным и обеспечить их информационную безопасность, включая разработку и принятие требований к техническим и программным средствам, используемым в информационной инфраструктуре этих объектов.

8. Необходимо совершенствовать законодательство об оперативно-розыскной деятельности в части:

создания необходимых условий для проведения оперативно-розыскных мероприятий в целях выявления, предупреждения, пресечения и раскрытия компьютерных преступлений и преступлений в сфере высоких технологий;

усиления контроля за сбором, хранением и использованием информации о частной жизни граждан, сведений, составляющих личную, семейную, служебную и коммерческую тайну.

9. Совершенствование уголовно-процессуального законодательства должно создать условия правоохранительным органам

оперативно и эффективно действовать в случаях угроз безопасности, осуществляемых с использованием ИКТ, к числу которых относятся коррупционные проявления с использованием цифровой валюты, единообразно оформлять доказательства, полученные с использованием компьютерных систем и телекоммуникаций.

Необходимо устранить правовую неопределенность в части использования работодателями средств визуального наблюдения, средств контроля телефонных переговоров, электронных сообщений, использования средств доступа в сеть «Интернет», поскольку эти средства могут быть использованы для противоправных действий.

Содержание

Разинкин А.В. Вступительное слово…… 3

Капинус О.С. Вступительное слово……. 7

Бессчасный С.А. Вступительное слово……... 12

Меркурьев В.В. Вступительное слово…….. 15

Доклады и выступления на пленарном заседании

Меркурьев В.В. Цифровые технологии в общей организации борьбы с преступностью…… 18

Сундиев И.Ю. «Токсичное» влияние цифросетевых структур на радикализацию молодежи……... 28

Хатов Э.Б. О роли цифровых технологий в анализе преступности……. 41

Исаенко В.Н. Прокурорский надзор за исполнением законов при расследовании преступлений в условиях развития компьютерных технологий…….. 47

Овчинский В.С. Об угрозах квантовых компьютерных вычислений…… 54

Выступления на секционных заседаниях

Секция 1. Использование цифровых технологий в общей организации борьбы с преступностью

Репецкая А.Л. Криптопреступления как следствие цифровизации преступности…… 61

Рогова Е.В. Роль информационно-коммуникационных технологий и компьютерной информации в совершении корыстных преступлений……. 68

Тисен О.Н. Доказывание преступлений, связанных с финансированием терроризма……... 73

Яковлева Л.В. Проблемы криминализации новых видов общественно опасных деяний, совершаемых с использованием информационно-телекоммуникационной сети «Интернет»…….. 77

Алтухов С.А. Проблемы борьбы с преступностью в условиях изменения формата медиапространства…….. 82

Горшенков А.Г., Горшенков Г.Г., Горшенков Г.Н. Криминологическая экспертиза и информационная безопасность…….. 88

Иванов П.И. Цифровая реальность и ее влияние на развитие оперативно-розыскной науки…….. 92

Алиуллов Р.Р., Иванов В.А. О некоторых факторах, способствующих совершению мошенничеств с использованием информационных технологий в банковской сфере…… 100

Воронин Ю.А. Основные тенденции преступности в цифровой сфере…….. 106

Швед Н.А. Цифровые технологии и уголовное право……... 112

Иванова Л.В. Уголовно-правовое противодействие киберпреступности в странах БРИКС……. 118

Забавко Р.А. О готовности российского уголовного права к использованию искусственного интеллекта при квалификации преступлений…… 122

Клочкова А.В. Влияние цифровой среды на формирование девиантного поведения подростков и молодежи……... 127

Никонов П.В. Роль информационно-коммуникационных технологий и компьютерной информации в совершении коррупционных преступлений, связанных с дачей и получением взятки и иными видами незаконного вознаграждения……. 132

Соколов М.А. Медиасреда как фактор криминализации молодежи…… 137

Пристанская О.В. Совершенствование законодательства в сфере противодействия кибербуллингу и другим видам психологического насилия в отношении несовершеннолетних посредством сети «Интернет»…… 142

Фещенко П.Н. К вопросу о личности «цифрового преступника» и его жертвы…….. 151

Маныч Е.Г. Кража финансовых данных или данных банковских карт – один из видов киберпреступления……. 156

Клименко А.К. Проблемы квалификации хищений, совершенных с использованием технологии бесконтактной оплаты…….. 159

Шевелева К.В. Об ответственности за реабилитацию нацизма в сети «Интернет». Вопросы терминологии…… 166

Баюш А.А. Экстерриториальность защиты прав субъектов персональных данных в рамках процесса цифровизации…. 171

Петрова Т.М. Уголовная ответственность за незаконные приобретение или продажу особо ценных диких животных, занесенных в Красную книгу, с использованием сети «Интернет»……. 176

Мурадян С.В., Кулиджанян Д.М. Особенности квалификации преступлений, совершенных с использованием информационно-коммуникационных технологий и в сфере компьютерной информации…… 180

Терехов М.Г. Межотраслевой институт цифровых активов: типологии криптовалют…… 186

Синолиц М.А. Уголовная ответственность за распространение ложной информации в сети «Интернет» о пандемии коронавирусной инфекции……. 190

Секция 2. Использование цифровых технологий в предупреждении преступности

Голубовский В.Ю. Проблемы предупреждения киберпреступности…… 195

Горошко И.В. Некоторые подходы к гармонизации национальных уголовных законодательств в сфере противодействия компьютерной преступности……. 200

Диканова Т.А. Цифровизация как фактор, способствующий предупреждению правонарушений в транспортной системе стран СНГ и ЕАЭС……. 205

Кунц Е.В. Зарубежный опыт противодействия преступлениям в сфере телекоммуникационных технологий……. 215

Дворецкий М.Ю. Направления совершенствования мер противодействия преступлениям в сфере компьютерной информации……... 220

Карлов И.В. Использование современных информационных технологий для противодействия преступности в местах лишения свободы…….. 223

Костенко К.А. О практике обеспечения информационной безопасности в системе СК России посредством мониторинга СМИ и информационно-телекоммуникационной сети «Интернет»…….. 230

Гаврилов Б.Я. Проблемы реализации отдельных положений уголовно-процессуального законодательства в условиях противодействия расследованию преступлений, совершаемых с использованием цифровых технологий……... 236

Гаврилин Ю.В. Научные основы преодоления противодействия расследованию преступлений, совершенных с использованием информационно-коммуникационных технологий…….. 241

Ережипалиев Д.И. Региональные подходы к обеспечению информационной безопасности детей……. 249

Колбая М.Б. Цифровые технологии как инструмент предупреждения насильственных преступлений, совершаемых на территории Республики Абхазия…… 255

Демидова-Петрова Е.В. Возможности Big Data в области предупреждения преступности несовершеннолетних……... 260

Михайлова Е.В. Криминологические аспекты преступлений в сфере компьютерной информации, совершаемых несовершеннолетними…….. 265

Винокуров С.И. Предупреждение сексуальной эксплуатации несовершеннолетних в сети «Интернет»…… 269

Александрова Л.И. Применение информационных технологий для противодействия преступлениям в таможенной сфере…….. 276

Зацепин М.Н., Зацепин А.М. Совершенствование криминологических механизмов противодействия преступности в условиях цифровой экономики……. 283

Тимошина Е.М. Противодействие самоубийствам несовершеннолетних, вызванным влиянием интернет-контента……. 293

Изгагина Т.Ю. Использование цифровой валюты в преступной деятельности и меры по противодействию криминальному рынку биткоина……. 298

Кондратюк С.В. Информационные источники следственной и судебной профилактики преступного занятия высшего положения в преступной иерархии…… 303

Коренюк А.Л. Современное состояние и тенденции учета преступлений в сфере компьютерной информации……... 308

Халиуллина Э.Т. Основные проблемы противодействия преступлениям, совершаемым с использованием персональных данных, и пути их решения……. 315

Россоловский П.А. Некоторые вопросы применения информационно-коммуникационных технологий в органах прокуратуры в контексте организации работы и управления…….. 321

Поливанов А.В. Криминологическое разграничение форм девиантного поведения треш-стрима и пранка…….. 325

Секция 3. Цифровые технологии в правоохранительной деятельности

Голоскоков Л.В. Правоохранительные органы в замкнутом круге цифровых и других высоких технологий……. 331

Зуев С.В. Цифровой правовой статус участника уголовного судопроизводства: понятие, признаки, содержание…….. 336

Беляева Л.И. Актуальные вопросы подготовки специалистов по информационной безопасности в высших учебных заведениях правоохранительных органов……... 343

Расторопова О.В. Применение интерактивных экспертных систем для выявления преступлений в сфере экономики (на примере кредитных преступлений)……... 348

Евдокимов К.Н. Противодействие компьютерной преступности в Российской Федерации: понятие, система, состояние, тенденции…… 354

Житников Б.Ю. Некоторые аспекты противодействия телефонному мошенничеству…….. 359

Киселёв Е.А. Особенности тактики проведения следственных действий при расследовании уголовных дел о преступлениях, совершаемых с использованием современных информационных и телекоммуникационных технологий……. 365

Кузнецов К.В. Использование программно-технических средств обеспечения анонимности пользователей в информационно-телекоммуникационной сети «Интернет» как одно из средств совершения преступлений повышенной латентности…… 370

Лебедева А.А. Расследование киберпреступлений следователями СК России…… 376

Раскина Т.В. Проблемы противодействия треш-стримам как пример необходимости изменения тактики обеспечения законности в сфере информационно-коммуникационных технологий…….. 380

Серова Е.Б. Некоторые проблемы доказывания по делам о преступлениях, совершенных с использованием высоких технологий……. 385

Шиханов В.Н. Уголовная статистика: подспорье в противодействии преступности или кладбище данных?.... 389

Шкеле М.В., Кузнецова Н.И. Ресурсы информационно-коммуникационных технологий в сфере противодействия экологической преступности…… 396

Колесникова Н.В. О некоторых проблемах государственного единого статистического учета данных о состоянии преступности с использованием ГАС ПС……. 401

Рубцова М.В. Органы прокуратуры в борьбе с киберпреступностью в России…….. 407

Вихляев А.А. К вопросу об использовании сотрудниками полиции личных технических средств при аудио- и видеофиксации противоправного поведения правонарушителей и о допустимости приобщения полученных результатов в качестве доказательств при производстве по делам об административных правонарушениях и в уголовном процессе……. 411

Прохоров А.Б. Некоторые аспекты использования электронных документов в уголовном судопроизводстве… 415

Винокуров М.В. Эффективность применения цифровых технологий в борьбе с фальсификацией лекарственных средств…… 421

Перина А.С. Проблемы уголовно-правовой оценки преступлений, совершаемых в сети Darknet…….. 427

Себякин А.Г. Принципы изъятия и криминалистического исследования информационных носителей…… 431

Федосеева А.А. Об актуальных проблемах организационного обеспечения раскрытия и расследования преступлений против конституционного права человека на неприкосновенность частной жизни, совершенных с использованием информационно-коммуникационных технологий…….. 436

Барчуков В.К. Применение элементов искусственного интеллекта в деятельности прокуратуры: современное состояние и перспективы…….. 440

Рекомендации конференции……. 445

Цифровые технологии в борьбе с преступностью: проблемы, состояние, тенденции

(Долговские чтения)

Сборник материалов
I Всероссийской научно-практической
конференции

(Москва, 27 января 2021 г.)

Подписано в печать 17.06.2021. Формат 60x90/16. Печ. л. 28,75.
Тираж 200 экз. Заказ 13.

Университет прокуратуры Российской Федерации
123022, Москва, ул. 2-я Звенигородская, 15