Кибермафия
Мировые тенденции и международное противодействие

Ю. Н. Жданов, С. К. Кузнецов,
В. С. Овчинский

Кибермафия
Мировые тенденции и международное противодействие

Вступительная статья
заместителя Секретаря Совета Безопасности
Российской Федерации,
председателя Межведомственной комиссии
Совета Безопасности Российской Федерации
по информационной безопасности
О. В. Храмова

НОРМА
Москва, 2022

УДК 343.9
ББК 67.51
Ж42

Рецензенты

Расторопов С. В. — доктор юридических наук, профессор (Университет прокуратуры Российской Федерации).

Осипенко А. Л. — доктор юридических наук, профессор (Краснодарский университет МВД России).

Ж42 **Жданов Ю. Н., Кузнецов С. К., Овчинский В. С.**

Кибермафия. Мировые тенденции и международное противодействие : монография / Ю. Н. Жданов, С. К. Кузнецов, В. С. Овчинский ; вступ. ст. О. В. Храмова. — Москва : Норма, 2022. — 184 с. — DOI 10.12737/1864981.

ISBN 978-5-00156-245-0 (Норма)
ISBN 978-5-16-110263-3 (ИНФРА-М, online)

В книге на основе анализа материалов ООН, Интерпола, Европола, других международных организаций рассматриваются тенденции развития организованной киберпреступности и механизмы международного сотрудничества в борьбе с ней.

Для широкого круга специалистов правоохранительных органов, студентов, преподавателей, аспирантов юридических вузов и всех интересующихся проблемами борьбы с киберпреступностью.

УДК 343.9
ББК 67.51

ISBN 978-5-00156-245-0 (Норма)
ISBN 978-5-16-110263-3 (ИНФРА-М, online)

К читателю

С развитием IT-технологий и Интернета вопрос ответственности за совершение киберпреступлений получил особую остроту во всем мире и в нашей стране. С 2013-го по 2021 г. уровень преступности с использованием высоких технологий вырос в России более чем в 20 раз. Сегодня каждое четвертое преступление в нашей стране совершается с помощью информационных технологий или в информационном пространстве.

Преступники посягают на различные сферы жизнедеятельности — имущественные права граждан, права личности, объекты критической инфраструктуры, причиняют ущерб коммерческим организациям и государству в целом. При этом их действия становятся все более агрессивными и организованными, злоумышленники принимают меры к тщательному сокрытию следов преступлений, к сохранению анонимности, продумывают свое поведение так, чтобы максимально осложнить сбор доказательств и избежать ответственности.

Современные преступники активно используют облачную инфраструктуру. Сегодня при совершении противоправных деяний применяются различные методы цифровой конспирации: шифрование данных, в том числе с использованием специализированных программ для маскировки IP-адресов, выход в Интернет через публичные точки доступа, использование учетных записей и идентифицирующих данных, принадлежащих иным лицам, не осведомленным о таком использовании.

Эксперты отмечают рост квалификации злоумышленников, усложнение их инструментария, повышение темпов использования новых уязвимостей, а также увеличение времени присутствия преступников в инфраструктуре. При этом преступники используют весь возможный арсенал средств (от VPN-программ до криптовалюты), чтобы сохранить свою анонимность и остаться безнаказанными.

Одним из ключевых направлений борьбы с преступным использованием информационно-коммуникационных технологий (ИКТ) является международное сотрудничество правоохранительных органов, которое приобретает особое значение при расследовании дел с признаками организованной преступной деятельности.

В нынешних условиях становится все более актуальным и востребованным знание современных мировых тенденций развития организованной преступности в информационной сфере, а также эффективных форм международного сотрудничества в борьбе с преступным использованием ИКТ.

В представленной Вашему вниманию монографии подробно рассматриваются открытые материалы Управления по наркотикам и преступности ООН, Интерпола, Европола, а также Всемирного экономического форума, посвященные анализу угроз, исходящих от организованных форм киберпреступности. Авторами дается оценка мировых тенденций организованной киберпреступности, ее структуры, формы и новых проявлений. Предлагается подробная криминологическая характеристика видов преступлений, совершаемых организованными группами. Особое внимание уделяется вопросам противодействия мошенничеству, вымогательству, шантажу в сети Интернет.

Рассмотренные авторами подходы, которые легли в основу докладов упомянутых международных организаций, дают возможность сопоставить их с позицией России и ее союзников в вопросах совершенствования борьбы с преступлениями с использованием ИКТ, в том числе в рамках международного сотрудничества.

Настоящую монографию дополняет проект конвенции ООН о противодействии использованию информационно-коммуникационных технологий в преступных целях, внесенный российской стороной в июле 2021 г. в учрежденный в ООН по инициативе России специальный межправительственный комитет экспертов открытого состава по разработке указанной всеобъемлющей универсальной конвенции.

Сравнительный анализ ключевых положений российского проекта и подходов других государств к решению проблем борьбы с преступным использованием ИКТ в контексте исследования путей формирования правовых основ системы обеспечения международной информационной безопасности мог бы стать следующим шагом авторов на данном направлении.

Полагаю, что представленные материалы заинтересуют политиков, ученых, сотрудников правоохранительных органов, профильных специалистов, которые профессионально погружены в проблематику информационной безопасности, а также студентов юридических вузов.

О. В. Храмов,
заместитель Секретаря
Совета Безопасности Российской Федерации,
председатель Межведомственной комиссии
Совета Безопасности Российской Федерации
по информационной безопасности

Введение

В докладе Всемирного экономического форума (ВЭФ) «О глобальных рисках 2022 года» отмечено, что государства, общество и компании все больше зависят от технологий в самых разных сферах — от предоставления государственных услуг до управления бизнес-процессами. Конвергенция технологических платформ, инструментов и интерфейсов в Интернете приводит к усложнению ландшафта киберугроз и увеличению числа критических точек отказа.

По мере того как общество все больше перемещается во все более децентрализованный цифровой мир (концепция «Web 3.0»), растет киберпреступность, из-за чего организации регулярно теряют десятки и даже сотни миллионов долларов. Но ущерб не только финансовый, под угрозой также критическая инфраструктура, социальное и психологическое благополучие граждан.

Растущая зависимость от цифровых систем за последние 20 лет радикально изменила жизнь людей. Вызванный COVID-19 переход к удаленной работе ускорил внедрение платформ и устройств, позволяющих передавать конфиденциальные данные третьим лицам — поставщикам облачных услуг, агрегаторам данных, интерфейсам прикладного программирования (API) и другим технологическим посредникам. Эти системы, будучи мощными инструментами для работы с данными, усиливают зависимость от поставщиков услуг. Удаленная работа привела к переносу цифровой информации из офисных сетей в домашние, где больше разнообразных подключенных устройств, а защита от несанкционированного доступа хуже. В то же время растет спрос на системы, где применяется несколько технологий, таких как искусственный интеллект, Интернет вещей/Интернет роботизированных устройств, блокчейн и 5G. Эти системы открывают перед бизнесом и обществом огромные возможности использования технологий, позволяют значительно повысить эффективность, качество и производительность, но они

же подвергают пользователей дополнительным, более опасным киберрискам.

В будущем взаимосвязь этих цифровых инструментов усилится по мере того, как общество будет переходить к следующей версии Интернета, построенной на технологии блокчейна. Одним из проявлений этой трансформации станет метавселенная — сеть трехмерных виртуальных пространств, созданная на базе криптовалют, уникальных токенов (NFT) и прочих технологий, обладающая беспрецедентной социально-экономической взаимосвязанностью и захватывающими возможностями виртуальной реальности. Пользователям придется ориентироваться в уязвимостях безопасности, обусловленных как повышением зависимости от сложных технологий, так и их растущей фрагментацией, децентрализацией и отсутствием структурированных защитных механизмов и комплексной инфраструктуры для обучения пользователей.

Люди все чаще становятся мишенями для атак, мошенничества, кибербуллинга и преследования, из-за чего они будут больше испытывать тревогу в отношении своих данных и их защиты. Наиболее уязвимы новые и будущие пользователи Интернета. Около 40% мирового населения пока не имеют к нему доступа. Но уже сейчас эти люди сталкиваются с неравенством в области цифровой безопасности, которое будет только расти с подключением к Интернету и метавселенной. В цифровых обществах уязвимые группы населения также чаще подвергаются цифровому риску.

Сайты по-прежнему используют разнообразные инструменты, которые позволяют отслеживать действия онлайн-пользователей. Новые риски для граждан могут создавать обязательные цифровые идентификаторы. В частности, все большую опасность представляют дипфейки (Deepfake), которые могут скомпрометировать биометрическую аутентификацию.

В условиях повсеместной зависимости от все более сложных цифровых систем нарастающие киберугрозы опережают возможности общества по эффективному управлению этими угрозами и их предотвращению. Например, цифровизация физических цепей поставок создает новые уязвимости, поскольку они зависят от поставщиков технологий и других сторонних организаций, которые также подвержены аналогичным угрозам.

Вредоносная деятельность расширяется из-за растущей уязвимости систем, а также из-за низкого риска наступления ответственности для киберпреступников. Группы «кибернаемников», ищущие наживы, готовы предоставить доступ к сложным инструментам взлома и таким образом облегчить проведение подобных атак. Кроме того, криптовалюты позволили киберпреступникам получать выкуп при относительно низком риске раскрытия и возврата денежных средств. Сами кибератаки также становятся более агрессивными и распространенными.

Киберпреступники, использующие программы-вымогатели, применяют все более жесткую тактику давления, а также выбирают более уязвимые цели, такие как коммунальные службы, системы здравоохранения и компании с большим объемом данных. Среди предлагаемых услуг — сбор информации о высших руководителях для последующего шантажа. Кроме того, доступ к продвинутым инструментам позволяет киберпреступникам успешно проводить не только массовые, но и целевые атаки, что в будущем может привести к еще большему финансовому, социальному и репутационному ущербу.

Киберпреступники активно подстраивают атаки по времени и выбирают периоды, когда специалисты по кибербезопасности и руководство компаний могут быть отвлечены на решение других важных задач, например во время пиковых вспышек COVID-19 или стихийных бедствий.

Также киберпреступники сегодня могут получать доступ к более качественной и конфиденциальной информации от жертв. А технология «дипфейк» позволяет злоумышленникам совершенствовать приемы социальной инженерии, распространять дезинформацию и сеять хаос в обществе, особенно в периоды высокой волатильности.

Нехватка специалистов, способных развивать кибербезопасность в организациях, грамотно тестировать и защищать информационные системы, а также обучать людей цифровой гигиене, превышает 3 млн человек. Как и в случае с другими ключевыми ресурсами, недостаток специалистов по кибербезопасности может в итоге препятствовать экономическому росту.

Существуют опасения, что мощности квантовых вычислений может хватить для взлома ключей шифрования. Это создает значительный риск безопасности в силу чувствительности и важности финансовых, личных и других данных, защищенных такими ключами. Возникновение метавселенной также может расширить возможности для атак злоумышленников, создав больше точек входа для вредоносных программ и утечки данных. Многочисленные формы цифровой собственности, такие как коллекционные предметы искусства на основе NFT и цифровая недвижимость, могут еще больше способствовать преступной деятельности.

По мере цифровизации ресурсов увеличивается риск кибершпионажа, который может не только нанести удар по репутации частных и государственных организаций, но и угрожать их дальнейшему развитию. Связь между цифровизацией и растущими киберугрозами также влечет за собой нематериальные последствия. Рост числа дипфейков и «дезинформации как услуги» может привести к усилению недоверия между обществом, бизнесом и правительством. Дипфейки могут использоваться для влияния на выборы или другие политические процессы.

Процветает рынок услуг, направленных на манипулирование общественным мнением в пользу клиентов, государственных и частных, или на нанесение ущерба конкурентам. По мере перехода банковских, медицинских и государственных услуг на дистанционные платформы станет легче осуществлять мошеннические операции, а следовательно, они будут происходить чаще.

Разрушительные кибератаки могут привести к финансовому краху организаций, которые не инвестируют в защиту цифровой инфраструктуры, особенно при реализации сценария, когда правительства запретят выкупы или введут наказания за ненадлежащий уровень кибербезопасности.

Компании должны действовать, предупреждая изменения в регулировании, поскольку скрытые тенденции в политике и геополитическая напряженность между различными странами могут повлиять на трансграничные потоки данных. Это может предполагать перенос обработки данных в юрисдикции, которые обеспечат более надежную защиту пользователей в вопросах конфиденциальности данных.

Разрозненные правоохранительные механизмы в разных юрисдикциях мешают борьбе правительств с киберпреступностью. Геополитические разногласия препятствуют потенциальному транс-

граничному сотрудничеству, поскольку правительства некоторых стран не хотят или не могут контролировать действия злоумышленников, которые совершаются внутри страны, но причиняют ущерб жертвам, находящимся за ее пределами.

Учитывая геополитическую напряженность вокруг цифрового суверенитета, неудивительно, что трансграничные кибератаки, дезинформация, а также искусственный интеллект оказались в числе областей, в которых международные усилия по снижению рисков наименее налажены и эффективны.

Киберугрозы приводят к дальнейшей разобщенности стран, правительства все больше принимают односторонние решения по контролю рисков. Атаки становятся все более серьезными и масштабными. Это еще больше усиливает напряженность между странами, которые стали жертвами киберпреступлений, и странами, которые причастны к их совершению. Кибербезопасность становится очередным камнем преткновения, а не основой для сотрудничества между государствами. Если не устранять киберугрозы, правительства будут продолжать принимать ответные меры против нарушителей (реальных или предполагаемых), что приведет к открытой кибервойне, дальнейшему разрушению общества и потере веры в способность власти управлять цифровым пространством.

Зарубежные компании по кибербезопасности прогнозируют рост глобальных затрат на защиту от киберпреступности и восполнение ущерба от кибератак на 15% в год, которые достигнут 10,5 трлн долларов США в год к 2025 г. по сравнению с 3 трлн долларов США в 2015 г.

Это представляет собой величайшее перераспределение экономического богатства в истории. В денежном выражении риск киберпреступности как стимул к инновациям и инвестициям экспоненциально больше, чем годовой ущерб, нанесенный стихийными бедствиями, киберпреступность выгоднее, чем мировая торговля всеми основными видами наркотиков в совокупности.

Приведенные цифры касаются только видимой части Сети. Помимо нее, в теневом Интернете ущерб от киберпреступности вообще не поддается количественной оценке. По некоторым данным, размер теневой сети (которая не индексируется и недоступна для поисковых систем) в 5000 раз превышает размеры официального Интернета.

Теневая сеть является местом, где киберпреступники покупают и продают вредоносное программное обеспечение (ПО), наборы эксплойтов и системы кибератак, которые они используют для нанесения кибердаров по жертвам, включая предприятия, органы власти, коммунальные структуры и поставщиков основных услуг.

Организованные криминальные формирования, занимающиеся киберпреступностью, объединяют усилия, а вероятность их обнаружения и судебного преследования оценивается в 0,05% согласно Отчету о глобальных рисках Всемирного экономического форума за 2020 г.

Применение новейших технологий — одна из главных особенностей современной организованной преступности. Преступники используют зашифрованную связь для контактов друг с другом, социальные сети и сервисы мгновенных сообщений для рекламы нелегальных товаров или распространения дезинформации. Интернет и электронная коммерция дают правонарушителям возможность получать доступ к информации и сложному современному инструментарию, облегчая совершение преступлений.

Хотя распространение дезинформации само по себе часто не является преступным поведением, оно может поощрять преступную деятельность или содействовать ее осуществлению. Так, мошенники и фальсификаторы инициировали кампании по распространению дезинформации в контексте пандемии COVID-19 для увеличения продаж своей продукции или для вовлечения жертв в мошеннические схемы.

Услуги киберпреступников можно приобрести, заплатив гонорар, абонентскую плату или процент от незаконной прибыли. В Интернете, особенно в теневом, широко предлагаются соответствующие криминальные инструменты, например вредоносное ПО, программы-вымогатели, средства поддержки фишинга, анализаторы трафика, устройства для кражи данных с кредитных карт и распределенные атаки типа «отказ в обслуживании» (DDoS), а также продаются зашифрованные данные кредитных карт лиц, ставших жертвами мошенничества.

Модель «преступление как услуга» делает криминальные услуги легкодоступными для любого желающего. Кроме того, интернет-платформы предоставляют инструкции по совершению большинства преступлений. Темы предлагаемых «руководств» и «учебных

пособий» самые разные: от производства синтетических наркотиков, изготовления примитивного огнестрельного оружия и самодельных взрывных устройств до всех видов киберпреступности.

Криптовалюты — средство оплаты нелегальных товаров и услуг. Децентрализация и полуанонимность обусловливают их привлекательность для осуществления преступных сделок. Мошенники особенно часто используют криптовалюты. Нелегальные доходы могут изначально иметь форму виртуальной валюты или могут быть конвертированы в цифровую форму. Новые методы отмывания денег с использованием криптовалют включают использование сервисов микширования и обмена монет.

Криминальный контент в Интернете сегодня доминирует в таких областях, как торговля, коммуникация и доступ к информации. Цифровая трансформация экономики, общества и частной жизни быстро прогрессирует и продолжит влиять на все аспекты жизни и деятельности человека. Неудивительно, что эти изменения оказали существенное влияние и на сферу организованной преступности. Практически все виды преступной деятельности теперь включают в себя онлайн-составляющие, такие как цифровые решения, облегчающие коммуникацию для преступников.

Информационно-коммуникационные технологии (ИКТ) изменили представления об организованной преступности. В частности, ИКТ оказали влияние на характер деятельности организованной преступности и типы групп, которые могут в ней участвовать. Некоторые традиционные ОПГ постепенно переходят от автономной преступной деятельности к киберпреступности.

Оргнизованные преступные группы все чаще стремятся сотрудничать с киберпреступниками, которые обладают важными навыками, необходимыми для выполнения криминальных кибероперациий.

Информационно-коммуникационные технологии также изменили способ структурирования и организации ОПГ. Они устраняют необходимость личного контакта между людьми и позволяют людям, которые никогда раньше не встречались, тесно сотрудничать и координировать свою деятельность из любой точки мира, используя псевдонимы. Таким образом, риск раскрытия своей личности и местонахождения другим членам ОПГ относительно невелик.

Помимо эволюции в структуре традиционных ОПГ наблюдается формирование «новых» групп, которые совершают киберпреступления и действуют частично, преимущественно или полностью в Сети. Эти группы демонстрируют поведение, сходное с поведением традиционных ОПГ, в частности используют их структуру и специальные процедуры, направленные на обеспечение анонимности членов и избежание обнаружения правоохранительными органами.

Информационно-коммуникационные технологии устранили барьеры для входа на незаконные рынки. Люди больше не ограничены географическим местоположением, они могут быть частью ОПГ из любой точки мира. ИКТ также предоставляют преступникам инфраструктуру, товары, персонал и клиентов, необходимых для участия в деятельности, связанной с организованной киберпреступностью. По этим причинам роль ИКТ в расширении незаконных рынков и сетей и создании более действенных незаконных бизнес-моделей является решающей.

Таким образом, проблема транснациональной организованной преступности усугубляется постоянно растущей глобальной связью и безграничной сферой киберпространства.

Часто понятие «организованная киберпреступность» заменяется термином «кибермафия». На наш взгляд, это допустимо, поэтому в нашей работе эти термины применяются как равнозначные.

В то время как общее количество исследований различных форм киберпреступности растет, исследований именно кибермафии намного меньше. Для восполнения этого пробела в нашей книге используются положения Обзора организованной киберпреступности, подготовленного Управлением по наркотикам и преступности (УНП) ООН в 2021 г., других материалов УНП ООН, докладов Европола «Оценка угрозы организованной преступности в Интернете (IOCTA)» (апрель и ноябрь 2021 г.), результаты исследований экспертов ВЭФ и других международных организаций, опубликованные в 2021 г. Кроме того, рассматриваются основные международные подходы к противодействию организованной киберпреступности.

Глава 1. Мировые тенденции кибермафии

1.1. Структура, организация и типы преступных групп, участвующих в организованной киберпреступности

Киберпреступность — это сложное понятие, охватывающее множество незаконных действий, направленных на ИКТ и (или) использующих ИКТ при совершении преступления.

Наряду с *чистой Сетью* (Surface Web), которая относится к видимой (или поверхностной) Сети и включает веб-сайты, индексирующиеся с помощью традиционных поисковых систем (Google, Bing и т. д.), киберпреступность пользуется *глубокой Сетью* (Deep Web), состоящей из сайтов, которые не отслеживаются традиционными поисковыми системами и, следовательно, недоступны для широкой публики. Сайты, расположенные в глубокой Сети, могут включать в себя сайты интрасети и сайты, защищенные паролем, а также сайты, для доступа к которым требуется специальное программное обеспечение.

Сайты, являющиеся частью глубокой Сети, к которым можно получить доступ только с помощью специального программного обеспечения, известны как сайты *темной (теневой) Сети* (Dark Net, даркнет).

Многие даркнет-сайты используют криптовалюты (биткойн, Monero и Ethereum) для финансовых транзакций. Популярность криптовалют привела к их использованию в мошенничестве, чтобы заманивать ничего не подозревающих инвесторов в мошеннические схемы. Криптовалюты используются преступниками для отмывания денег. Криптовалюты — это не только инструмент, используемый ОПГ, но и цель этих преступников. Например, так называемая группа Байроба занималась «криптоджекингом», злонамеренным майнингом криптовалют, при котором вредоносный код использовался для заражения систем и использования ресурсов зараженных систем для добычи криптовалют.

Что сегодня представляют собой киберпреступники?

В исследовании 2019 г., основанном на данных, извлеченных из пресс-релизов Министерства юстиции США (выборка составила 225 киберпреступников из разных стран по 123 делам, связанным с 414 киберпреступлениями), раскрыт профиль транснационального киберпреступника. Одновременно исследован групповой элемент, в котором киберпреступники участвуют как члены международных сетей организованной преступности.

Средний возраст преступников — 35 лет. Мужчины составляли 94% преступников (212 из 225). Среднее количество фигурантов киберпреступной деятельности — пять человек. Установлено, что более 68% обвиняемых работают в группах, а не самостоятельно. Это важный результат, так как многие воспринимают киберпреступников как «волков-одиночек», занимающихся хакерской деятельностью. На самом деле *киберпреступники с легкостью присоединяются к международным организованным преступным сетям на обширном пространстве кибермира.*

В ходе еще одного исследования социологической структуры и организационной практики киберпреступников (изучено 18 групп преступников из Нидерландов, которым были предъявлены уголовные обвинения за вредоносные ПО и фишинговые преступления против банков и компаний, выпускающих кредитные карты) ученые обнаружили: ни в одной из криминальных сетей, участвовавших в этом исследовании, не было одиночек. Большинство сетей, которые исследователи категорически определили как команды, имели иерархическую структуру. Они также длительное время совершали преступления. Основные члены команды отвечали за планирование кибератаки, другие, которые обладали определенными знаниями или навыками, использовались для проведения атак, остальные — для покупки вредоносных программ или похищенных кредитных карт.

Например, в конце октября 2021 г. в ходе международной полицейской операции, в которой принимала участие Германия и семь других стран, была вскрыта сеть кибервымогателей, которая предположительно совершила компьютерные атаки на компании в десятках стран с целью получения выкупа. После двухлетнего расследования были арестованы 12 подозреваемых в Украине и Швейцарии.

По данным Европола, в 2020 г. жертвами вымогателей стали около 1800 компаний в 71 стране. Члены преступной группировки получали доступ к IT-системам фирм с помощью так называемых фишинговых электронных писем и другими способами. Затем они при помощи вирусов-вымогателей (ransomware) блокировали фирмам доступ к документации, шифруя его, и требовали выкуп за предоставление ключа для расшифровки.

Как отмечают международные эксперты, современная киберпреступность — это не привычная мафия, а нетрадиционная организованная преступность. И инструменты борьбы с ней (правовые и организационные) должны также быть адекватны новому явлению.

По данным УНП ООН, в киберсреде различаются ОПГ с иерархической структурой, с некоторой формой централизации, разделения труда и идентифицируемых лидеров и изменчивые, непостоянные, слабо аффилированные и децентрализованные группы. Одни ОПГ используют онлайн-форумы и платформы для регулирования и контроля над предоставлением незаконных товаров и услуг. Другие ОПГ имеют структуры по предоставлению услуг (т. е. предлагают преступление как услугу).

Например, Shadowcrew, международная преступная организация, насчитывающая около 4000 членов, продвигала и содействовала широкому спектру преступных действий в Интернете, включая кражу в электронном виде личной информации, мошенничество с кредитными и дебетовыми картами, а также изготовление и продажу фальшивых документов, удостоверяющих личность.

Подобные группы демонстрируют поведение, аналогичное поведению традиционных ОПГ, в частности использование структуры и процедур, которые предназначены для сохранения анонимности членов и ухода от внимания правоохранительных органов путем развертывания оперативных мер безопасности для сокрытия их личности и действий. Эти группы также принимают меры для уклонения от обнаружения правоохранительными органами. Фактически форумы с материалами о сексуальном насилии над детьми и специализированные форумы для киберпреступников обычно применяют более строгие меры безопасности, чем те сайты, которые предлагают наркотики и другие незаконные товары.

Например, Dreamboard, незаконный сайт, на котором обменивались материалами о сексуальном насилии над детьми, чтобы предотвратить проникновение со стороны правоохранительных органов, требовал от всех своих участников пройти проверку и постоянно размещать на платформе материалы о сексуальном насилии над детьми. Администратор Card Planet (кардинг-форум, где данные кредитных карт, которые были украдены преимущественно в результате компьютерных вторжений, предоставлялись за определенную плату) также создал сайт под названием Cybercrime Forum для элитных киберпреступников. Любой человек, заинтересованный в использовании этого сайта, должен был быть проверен тремя действующими членами и уплатить взнос (обычно 5000 долларов США в качестве страховки). Затем участники сайта голосовали за то, следует ли предоставить потенциальному члену доступ к сайту. Cybercrime Forum принял и другие меры безопасности, чтобы избежать обнаружения правоохранительными органами. Например, блокировался доступ к сайту арестованным участникам, чтобы не дать правоохранительным органам использовать их в своих целях.

Организованные преступные группы в киберсреде можно разделить:

— на группы, которые преимущественно действуют онлайн и совершают киберпреступления;

— группы, которые действуют как офлайн, так и онлайн;

— группы, которые преимущественно работают в офлайн-режиме и занимаются киберпреступностью, чтобы расширить и облегчить свою деятельность.

Существуют два типа *групп, которые преимущественно действуют в Сети и совершают киберпреступления*: рой и хабы.

Рой можно охарактеризовать как объединение в течение ограниченного периода времени отдельных лиц для выполнения конкретных задач с целью совершения киберпреступления. После того как они выполнят поставленную задачу и преуспеют в совершении киберпреступления как коллектив, некоторые, большинство или все участники могут пойти своим путем, а временная группа, которая была сформирована, может быть распущена. Это расформирование не препятствует тому, чтобы кто-либо из лиц стал частью другого

роя и участвовал в аналогичных или иных киберпреступлениях в будущем с теми же или с другими лицами.

Рои характеризуются как децентрализованные сети, обычно (хотя и не исключительно) состоящие из «эфемерных групп индивидов» с общей целью и минимальными цепочками подчинения.

Примером состава роя является группа «хактивистов» Anonymous. Хотя у Anonymous нет заявленного лидера, у группы есть некоторая степень лидерства, по крайней мере в том смысле, что есть члены группы, которые берут на себя инициативу в организации, планировании и в итоге в принятии решений о совершении киберпреступлений.

В большинстве юрисдикций рои не считаются ОПГ, если они не занимаются киберпреступностью для получения материальной выгоды.

Хаб — это группа, основная часть которой состоит из преступников, окруженных периферийными криминальными партнерами. Хаб более структурирован, чем рой, он имеет командную структуру, которую можно идентифицировать. Обычно *деятельность хабов направлена на получение прибыли.* Некоторые из преступных действий, соответствующих этой организационной структуре, включают фишинг, сексуальные преступления и операции с вредоносными программами (черви, вирусы, пугающее ПО).

Пример хаба — Dreamboard — преступное предприятие, состоявшее из электронной доски объявлений, которая рекламировала и распространяла материалы о сексуальном насилии над детьми только среди своих членов. Чтобы присоединиться к Dreamboard, потенциальные участники должны были предоставить материалы о сексуальном насилии над детьми. Чтобы оставаться членами Dreamboard, участники должны были постоянно предоставлять материалы о сексуальном насилии над детьми. Доступ участника аннулировался, если он в течение 50 дней не публиковал материалы о сексуальном насилии над детьми. Члены Dreamboard соблюдали правила, которые были изложены на четырех языках (английском, японском, русском и испанском). Одно из правил заключалось в том, что на сайте должны быть представлены материалы, в которых изображены девочки не старше 12 лет.

Администратор Dreamboard разместил участников в отдельных группах. Члены группы SuperVIP были доверенными участниками сайта, которые производили и рекламировали свои собственные материалы о сексуальном насилии над детьми. Члены группы SuperVIP имели больший доступ к материалам сексуального насилия над детьми, чем другие участники. Члены группы VIP и другие участники имели более ограниченный доступ к материалам сексуального насилия над детьми. Чтобы перейти на более высокий уровень, им необходимо было производить материалы о сексуальном насилии над детьми и предоставлять их другим участникам, размещать больше рекламы с материалами о сексуальном насилии над детьми, которых у других участников еще не было.

Несколько членов Dreamboard были приговорены к пожизненному заключению за свои преступления.

Группы, которые действуют в офлайн- и онлайн-режиме и участвуют в преступлениях и киберпреступлениях, известны как *гибриды.* Такие группы имеют две категории: кластерные гибриды и расширенные гибриды. Как и хабы, *эти группы в основном ориентированы на получение прибыли.*

Кластерный гибрид относится к группе, которая занимается определенными видами деятельности и (или) использует определенные методы для совершения киберпреступления. Кластерный гибрид имеет структуру. Его отличает способность выполнять свои операции как онлайн, так и офлайн. Эти группы часто сосредоточены на конкретных преступлениях и киберпреступлениях, используют определенную тактику, имеют идентифицируемый метод работы и (или) действуют в определенном месте.

Типичным примером кластерной гибридной группы является группа, которая занимается скиммингом (незаконное считывание банковских карт) банкоматов, а полученные данные использует для совершения покупок в Интернете или продает на форумах.

Кластерные гибридные группы участвуют и в других формах мошенничества. Например, ОПГ из Великобритании совершила международное мошенничество в Интернете в отношении лиц в США, рекламирующих арендуемую недвижимость. В частности, члены кластерной гибридной группы, используя поддельные идентификационные данные, притворя-

лись заинтересованными арендаторами, связывались с частными лицами, рекламирующими недвижимость, и предлагали им деньги (например, задаток и арендную плату). Если намеченные лица отвечали, преступники отправляли в виде поддельного кассового чека деньги в сумме, превышающей запрашиваемую. Затем преступники связывались с людьми, заявляли, что лишние деньги были отправлены случайно, и просили отправить им их через известную службу денежных переводов. В некоторых случаях преступники убедили людей отправить денежным переводом всю сумму чека.

Расширенный гибрид более сложен, менее централизован и имеет менее очевидное ядро, чем кластерный гибрид. Расширенные гибриды состоят из единомышленников и подгрупп, которые осуществляют различную преступную деятельность. Они не так хорошо определены, как кластерные гибриды, и их состав более сложен.

Сообщества рынка даркнета (такие как Silk Road, Silk Road 2.0 и Dream Market), в которых есть администраторы и модераторы (контролирующие и управляющие сайтами), продавцы (продающие незаконные товары и услуги — наркотики, поддельные документы и деньги, инструменты для компьютерного взлома), покупатели (покупающие незаконные товары и услуги) и поставщики, слабо взаимосвязаны и могут быть классифицированы как расширенные гибриды.

Некоторые сообщества даркнета, которые сосредоточены на одном киберпреступлении и не столь сложны по своему составу, могут также считаться кластерными гибридами.

Некоторые ОПГ в основном *действуют в офлайн-режиме* и используют ИКТ только для расширения или поддержки незаконной деятельности и операций. Эти группы имеют иерархическую структуру, обычно состоят из традиционных ОПГ и стремятся за счет Интернета расширить такую незаконную деятельность, как азартные игры, вымогательство, проституция и торговля людьми.

Члены и сотрудники «Семьи Гамбино из Коза Ностры» в США осуществили интернет-схему с участием развлекательных сайтов для взрослых с целью обмана посетителей этих сайтов. Бесплатные туры, рекламируемые на сайте, использовались, чтобы побудить посетителей ввести данные своей кредитной карты под предлогом того, что это необходимо для подтверждения их возраста. Затем данные кредитной карты использовались для совершения мошеннических транзакций.

Роли внутри ОПГ в киберсети различаются в зависимости от совершенного киберпреступления и выполнения задач, связанных с незаконными действиями или достижением целей группы. Роли лиц, совершающих межличностные киберпреступления, такие как сексуальное насилие и эксплуатация детей в Интернете, отличаются от ролей групп, которые преимущественно занимаются киберзависимыми преступлениями.

Организованные преступные группы в киберсети, которые в основном совершают межличностные киберпреступления, назначают членам определенные роли, такие как выявление, вербовка и в итоге побуждение несовершеннолетнего к половому акту или выявление, создание, получение и распространение материалов о сексуальном насилии и эксплуатации детей.

Участники таких ОПГ имеют определенные роли, связанные с инструментами и технологиями, необходимыми для совершения киберпреступлений, например:

— *кодировщики* — лица, ответственные за разработку вредоносных программ, эксплойтов (программ или фрагментов кода, предназначенных для поиска и использования недостатков безопасности или уязвимостей в приложении или компьютерной системе) и других инструментов, используемых для совершения киберпреступлений (например, они могут создавать собственные эксплойты для платежей);

— *хакеры* — лица, ответственные за использование уязвимостей в системах, сетях и приложениях;

— *техническая поддержка* — лица, обеспечивающие техническую поддержку деятельности группы, включая обслуживание инфраструктуры и используемых технологий;

— *хосты* — лица, которые осуществляют незаконную деятельность на серверах или в офлайне, чтобы избежать обнаружения правоохранительными органами, а также обеспечить непрерывность незаконных действий. Эти роли часто определяются в ОПГ, которые предоставляют преступление как услугу.

Помимо взлома, вредоносного ПО и хостинга предлагаемые незаконные услуги включают предоставление наборов инструментов для эксплуатации или информацию об уязвимостях системы и способах использования этих уязвимостей, а также учебные пособия по различным киберпреступлениям;

— *специалисты* — лица, которые специализируются на конкретном киберпреступлении, тактике или методе его совершения. Примером специалиста является человек, который разрабатывает «шифровальщики» — программные инструменты, которые шифруют вредоносное ПО, чтобы оно не было обнаружено антивирусными программами на устройствах;

— *поставщики и распространители незаконных товаров и услуг:*

«обналичители» — лица, которые конвертируют незаконные товары в деньги;

«денежные мулы» (или *«бегуны»*) — лица, которые могут использоваться для вывода средств, или перевода денег онлайн, или получения наличными в банке.

Роли внутри ОПГ в киберсреде меняются, и лица, выполняющие эти роли, участвуют в группе только до тех пор, пока не выполнят свою задачу.

Некоторые члены группы могут считаться «расходным материалом». Например, «денежные мулы», которых находят в Интернете и просят открыть банковские счета (или использовать их собственные счета) и получать деньги от других (или отправить по почте, или физически перемещать посылки, получая их и пересылая, отправляя или доставляя в пункт назначения), часто рассматриваются группой как «расходный материал» (особенно если они невольно участвуют в этой деятельности).

Роли в ОПГ различаются в зависимости от пола. Преступники-мужчины преимущественно занимают руководящие должности, в то время как женщины в основном выполняют другие функции (вербовщиков, кодировщиков, специалистов и организаторов). Однако из этого правила есть и исключения.

Виновные в организованных киберпреступлениях могут быть частью группы, участники которой находятся в географической близости. Исследования показали, что географическая близость между преступниками сыграла определенную роль в формировании и расширении ОПГ. Тем не менее многие ОПГ образуются и процветают даже в тех случаях, когда географическая близость между их членами не имеет принципиального значения или вовсе отсутствует. Например, участники даркнета (администраторы, модераторы, продавцы, покупатели и поставщики) могут быть из любой точки мира.

1.2. Виды организованной киберпреступности

Киберзависимые преступления нацелены на ИКТ и были бы невозможны без использования этих технологий. Киберзависимые преступления имеют цель нарушить конфиденциальность (доступ ограничен авторизованными пользователями), целостность (данные верны, надежны и действительны) и ограниченную доступность (системы и данные доступны по запросу) компьютерных систем и данных. Незаконные действия против конфиденциальности, целостности и доступности компьютерных систем и данных включают незаконный доступ к компьютерной системе и (или) компьютерным данным; незаконный перехват компьютерных данных и (или) получение компьютерных данных; внедрение незаконных данных, вмешательство системы и незаконное производство, распространение, использование и владение компьютерными инструментами ненадлежащего использования.

Эти киберпреступления совершаются по разным причинам, включая финансовые, идеологические, политические и личные (например, месть, личное удовлетворение, получение статуса и признание среди сверстников).

Незаконный доступ. Несанкционированный или незаконный доступ к ИКТ и (или) его данным широко известен как *взлом*. Под взломом понимается не только получение несанкционированного или незаконного доступа, но и превышение разрешенного доступа. Оба эти действия запрещены законом, но действие этого запрета зависит от страны и региона.

Незаконный доступ может быть получен различными способами, например с помощью вредоносных программ и других инструментов для эксплуатации уязвимостей системы, а также с помощью социальной инженерии, разработанной для того, чтобы заставить ничего не подозревающих людей совершить действия в

интересах преступников (например, раскрыть личную информацию или перейти по ссылке, зараженной вредоносным ПО).

Хакеры могут получить доступ или попытаться получить доступ к системам и данным; превышать или пытаться превысить разрешенный доступ к системам и данным; могут использовать этот доступ для кражи, изменения, нарушения или иного повреждения систем и данных. Что касается последнего, то, как только хакеры получают незаконный или несанкционированный доступ к системам, они могут просматривать, загружать, изменять или красть данные, повреждать системы или прерывать, блокировать доступ к системе и данным законных пользователей.

Незаконный перехват или захват. Многосторонние, региональные соглашения и национальные законы о киберпреступности запрещают незаконный перехват или получение компьютерных данных. Не существует универсального определения незаконного перехвата или получения компьютерных данных, и определения, включенные в законы, различаются.

Так, Соглашение о сотрудничестве государств — участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации от 1 июня 2001 г. призывает к криминализации: незаконного доступа к компьютерной информации, защищенной законом, если таковое действие приводит к разрушению, блокировке, изменению или копированию информации или нарушению функционирования компьютера, компьютерной системы или связанных сетей.

Киберпреступлениями, мешающими работе систем, являются атаки типа *«отказ в обслуживании»*. Распределенная атака «отказ в обслуживании» стремится перегрузить ресурсы цели, чтобы предотвратить законный доступ к цели. Вместо одного компьютера или одной технологии одновременно используются несколько компьютеров и технологий для того, чтобы превысить способность атакуемого сайта обрабатывать запросы. Распределенные атаки типа «отказ в обслуживании» могут быть совершены несколькими пользователями со своих устройств с целью скоординированных кибератак или с нескольких компьютеров и других устройств, зараженных вредоносным ПО, использующихся для проведения кибератак.

Сеть цифровых устройств, зараженных вредоносным ПО, которое может использоваться в распределенной атаке типа «отказ в обслуживании», представляет собой так называемый *ботнет*. Вредоносная программа, используемая для создания ботнета, позволяет отслеживать и удаленно управлять зараженными цифровыми устройствами.

Злоумышленники распределенных атак типа «отказ в обслуживании» используют существующие инструменты для проведения таких атак, комбинируют существующие инструменты, настраивают существующие инструменты и создают новые. Эти инструменты могут быть сделаны по индивидуальному заказу, или существующие инструменты изменяют в соответствии с предпочтениями пользователей. Доступ к этим ботнетам, а также к другим системам и данным о целях также предлагается ОПГ в режиме онлайн в качестве платной услуги (иногда называемой «доступ как услуга»).

Торговля наркотиками в Сети. Веб-сайты, онлайн-магазины, тематические объявления, платформы и приложения социальных сетей используются в рекламе, продаже и покупке наркотиков в Интернете.

Торговля оружием в Сети. Огнестрельное оружие рекламируется и продается в клирнете (чистом, обычном Интернете) и в даркнете. В клирнете веб-сайты, чаты, форумы, платформы социальных сетей, онлайн-рынки и сайты классической рекламы используются для запроса, рекламы и продажи огнестрельного оружия. Огнестрельное оружие может рекламироваться и продаваться на сайтах клирнета на законных основаниях или в нарушение существующих законов и условий обслуживания веб-сайтов.

В даркнете огнестрельное оружие рекламируется и продается преимущественно через крипторынки (сайты, похожие на сайты известных онлайн-торговых предприятий, и сайты продавцов, где продавцы продают свои собственные товары или услуги). Техническая информация и другие данные, относящиеся к разработке, сборке, приобретению и использованию огнестрельного оружия, также размещаются в клирнете и даркнете.

Нередко наряду с продажей оружия преступники оказывают комплекс криминальных услуг.

Теневой веб-форум под названием «Deutschland im Deep Web — Keine Kontrolle, alles erlaubt!» («Германия в глубокой сети — никакого контроля, все разрешено!») был создан зло-

умышленником, который действовал под именем пользователя «luckyspax». С 18 марта 2013 г. до своего ареста 8 июня 2017 г. обвиняемый действовал в качестве единственного администратора этого форума в даркнете, проживая в Германии. Форум, созданный в сети Tor через домен germanyhusicaysx.onion, использовался в основном для обсуждений и (преимущественно публичного) обмена сообщениями, а также для проведения незаконных продаж. Чтобы активно использовать платформу форума, необходимо было зарегистрироваться под именем пользователя и предоставить зашифрованный адрес сообщения. До своего закрытия 8 июня 2017 г. платформа была одним из крупнейших подпольных форумов в Германии с более чем 23 тыс. зарегистрированных пользователей.

Обвиняемый разделил платформу на разные тематические категории, которые были предназначены для обмена информацией по определенным темам или сделок купли-продажи: религии (исламисты, христианские фундаменталисты, судный день); свобода (свобода слова, воли и подавления); спорт (боевые искусства, бодибилдинг, стероиды и допинг); политика и экономика; глубокая сеть: общие темы о глубокой сети; вебсайты (обзор и обсуждение скрытых услуг); учебные пособия (на немецком языке по Tor, скрытым службам, шифрованию и т. д.); биткойны (спекуляция, анонимизация и торговля); безопасность информационных технологий; «детская площадка» (грабежи и т. д.); мошенничество и обман (мошенничество, кардинг и преступление); оружие (производство, распространение и надлежащее использование); эротика (секс, предпочтения, отношения и проституция); самоубийство (последствия, обмен опытом и сам акт); наркотики (общие темы о наркотиках и лекарствах): отчеты и советы по опыту (более безопасное использование, отчеты о поездках, мнения), выращивание и производство (обмен опытом, проблемами и помощью), исследовательские химические вещества (опыт, проблемы, ингредиенты и законность), торговая площадка: подтвержденное предложение (каннабис, стимуляторы, психоделики, аптеки), предложение (каннабис, стимуляторы, психоделики, аптека, новые услуги и программное обеспечение); поиск (услуги, товары, информация и т. д.); зона свободной торговли (корзина); обмен контактами (заинтересованы в новых контактах?); отчеты об опыте и обзоры (относительно предложений здесь или на других торговых площадках).

Общение на платформе в основном происходило через форумы, которые были доступны каждому пользователю и лишь частично зашифрованы. Кроме того, пользователи могли общаться с помощью функции внутреннего обмена личными сообщениями, которые в обязательном порядке зашифровывались с использованием стандартной системы шифрования. Сообщения старше одного месяца автоматически удалялись. Пользователи также могли общаться через хорошо известный протокол зашифрованной связи или в режиме реального времени через службу обмена сообщениями, которая требовала от пользователей наличия отдельного приложения для обмена мгновенными сообщениями. Кроме того, для транзакций, совершаемых на платформе, была предложена услуга условного депонирования.

Создатель платформы не получал долю прибыли от продаж на платформе. Использование услуги условного депонирования также не основывалось на плате. Платформа и ее создатель финансировались исключительно за счет пожертвований в биткойнах. 24 декабря 2015 г. обвиняемый получил 9850 евро в виде пожертвований. Властям удалось установить его личность после его обращения за пожертвованиями. Платформа использовала биткойн в качестве виртуальной валюты, а пожертвования переводились на биткойн-адрес. Через обмен биткойнов эти пожертвования могли быть переведены обратно в фиатную валюту. Биткойны были переведены обратно в фиатную валюту через Bitcoin.de, где обвиняемый использовал свое настоящее имя и, следовательно, мог быть идентифицирован.

С 27 сентября 2015 г. по 18 августа 2016 г. обвиняемый разместил в Сети не менее 15 рекламных текстов от пользователей о продаже наркотических средств. Он также переместил существующие и ранее выпущенные им рекламные объявления из подкатегории «Предложение» в подкатегорию «Предложение подтверждено» и пометил каждого соответствующего продавца как «Подтвержденного продавца». Создав категорию «Оружие» на форуме, он также поддерживал торговые операции с оружием с 11 февраля 2015 г. до своего ареста в июне 2017 г. Ни у обвиняемого, ни у пользователей форума не было соответствующего разрешения на торговлю наркотическими средствами или оружием. Транзакции, проводимые через платформу, включали продажу пистолета и соответствующих боеприпасов пользователем «rico» пользователю «Maurächer».

Используя приобретенное оружие, Maurächer 22 июля 2016 г. совершил массовую стрельбу в торговом центре, в результате чего девять человек погибли и пятеро получили серьезные ранения. В связи с продажей оружия Maurächer был признан виновным по девяти пунктам обвинения в убийстве по неосторожности и пяти пунктам обвинения в нанесении телесных повреждений и приговорен к семи годам лишения свободы.

Создателю платформы было предъявлено обвинение в содействии незаконной рекламе наркотических средств, содействии преднамеренной незаконной торговле огнестрельным оружием, содействии умышленному незаконному приобретению полуавтоматического пистолета и умышленному незаконному приобретению наркотических средств. Ему также было предъявлено обвинение в пособничестве умышленной незаконной торговле огнестрельным оружием в сочетании с убийством по неосторожности и нанесением телесных повреждений по неосторожности в связи с продажей оружия, использованного для проведения массового расстрела. Он был приговорен к шести годам лишения свободы.

Торговля объектами дикой природы в Сети. Интернет-торговля объектами дикой природы растет. Чаще всего она происходит на платформах социальных сетей.

В 2020 г. в ходе анализа незаконных торговых площадок, действовавших в Великобритании, обнаружено 1194 рекламных объявления, в которых продавалось 2456 объектов дикой природы на общую сумму в 1 млн долларов США.

Торговля культурными ценностями в Сети. ОПГ занимаются незаконным оборотом культурных ценностей через законные онлайн-рынки и надежные аукционные сайты, а также через подпольные незаконные рынки. Социальные сети и коммуникационные приложения также используются для незаконного оборота культурных ценностей. Переход к онлайн-торговле расширил потенциальную клиентскую базу, создал новые рынки для малых, недорогих предметов, таких как монеты, которые раньше было невыгодно продавать.

Власти, расследующие незаконный оборот культурных ценностей в Интернете, сталкиваются с рядом проблем, в том числе с разнообразием платформ, на которых торгуют имуществом, отсутствием информации, помогающей правильной идентификации предметов, трудностями с идентификацией продавцов. Чтобы избежать обнаружения, торговцы культурными ценностями, действующие в Сети, используют хакерские методы, такие как подделка IP-адреса (т. е. замена известного IP-адреса поддельным).

Отмывание денег в Сети. Процесс отмывания денег состоит из трех этапов: размещение, расслоение и интеграция. На этапе размещения незаконно полученные деньги распределяются в финансовой системе (например, путем покупки активов или обмена валюты). Следующий этап, многоуровневый, включает в себя множество действий, направленных на дальнейшее удаление доходов, полученных от преступной деятельности, от их первоначального источника, что затрудняет раскрытие отмывания денег. В частности, как только доходы от преступления были помещены в финансовую систему, они перемещаются в другие финансовые учреждения или конвертируются из одного типа активов в другой. Наконец, доходы от преступной деятельности возвращаются в экономику. На этом этапе отмывания денег и интеграции доходы от преступления кажутся законными и используются преступниками для покупки собственности или приобретения других активов. Часто ОПГ конвертируют деньги в биткойны, передавая биткойны членам и партнерам в других странах. Одновременно партнеры используют биржи биткойнов для конвертации биткойнов в фиатную валюту. Для сбора, выкупа и конвертации часто используется третья сторона.

Многие законные криптовалютные биржи ужесточили свои правила «знай своего клиента» (KYC). К сожалению, отмывание криптовалюты остается возможным из-за биткойн-миксеров[1], сервисов обмена и бирж, работающих в «серых» зонах. Киберпреступники также могут использовать законных провайдеров VPN[2], поскольку они обеспечат им безопасный и надежный просмотр веб-страниц. Эти компании по-прежнему выполняют законные запросы о предоставлении информации, когда их услуги используются для киберпреступной деятельности.

Азартные игры в Интернете. Это предложение игр в казино (например, покер) или ставок (например, на скачках и спортивных

[1] Сервис, усложняющий отслеживание транзакций.

[2] Virtual Private Network — виртуальная частная сеть. Технология, позволяющая скрыть информацию о пользователе сайтом.

мероприятиях) в Интернете. Веб-сайты и контент, посвященные азартным играм в Интернете, доступны на нескольких языках и предлагают широкий выбор валют и способов оплаты. У традиционных (офлайн) игорных заведений, таких как казино и букмекерские конторы, есть определенные язык, валюта и варианты оплаты, которые зависят от географического положения заведения.

Основное различие между традиционными азартными играми и азартными играми в Интернете заключается в том, что человек может участвовать в азартных играх в Интернете в любое время и в любом месте, независимо от географического положения. Услуги интернет-гемблинга могут быть предоставлены традиционными казино, или букмекерскими конторами и организациями, у которых нет традиционных казино, или букмекерскими конторами, которые имеют только удаленные игровые услуги.

Тип азартных игр, которые считаются незаконными, варьируется в разных странах. Из-за различий в законах ОПГ могут размещать серверы и вести свою деятельность в юрисдикциях, где азартные игры в Интернете являются законными. У них может быть штаб-квартира в одной стране, серверы в другой или нескольких других странах и центры поддержки в разных странах, в зависимости от законов каждой страны в отношении Интернета.

1.3. Новые проявления организованной киберпреступности

Новая реальность, вызванная глобальной пандемией, требует быстрой адаптации, и вполне вероятно, что темп и организация личной и профессиональной жизни навсегда изменились. Неизбежно эти события также стимулируют к инновациям киберпреступников, которые стремятся извлечь выгоду из новых возможностей.

В ноябре 2021 г. на сайте ВЭФ опубликовано сразу несколько тревожных материалов о тенденциях киберпреступности и состоянии кибербезопасности.

Цифровизация преступности. Методы и инструменты, используемые киберпреступниками, все чаще применяются в других областях преступности, а цифровая криминальная экосистема продолжает развиваться тревожными темпами. Конфиденциальность

и удобство, предлагаемые цифровыми платформами, и криптовалюты выгодны при любой незаконной деятельности.

Операторы *вредоносных программ для мобильных устройств* воспользовались ростом онлайн-покупок, используя службы доставки в качестве фишинговых приманок, чтобы обманом заставить своих жертв загрузить свой вредоносный код. Таким образом крадутся учетные данные или совершаются различные формы мошенничества с доставкой.

Трояны мобильного банкинга стали особенно серьезной угрозой из-за возросшей популярности мобильного банкинга.

Преступники продолжают использовать пандемию COVID-19 для *онлайн-продажи поддельной медицинской продукции* и стремятся украсть учетные данные.

Анонимность в Интернете усугубляется широким распространением *технологий шифрования*, которые могут принести пользу и законным пользователям, и преступникам. Международные правоохранительные органы пристально следят за поставщиками VPN и криптографических телефонов (криптофонов), которые обслуживают криминальные элементы.

Преступление как услуга. Модель «преступление как услуга» (Crime-as-a-Service, CaaS) остается важной чертой киберпреступного подполья и является сквозным фактором во всех областях киберпреступности. Доступные эксплойты и другие подобные услуги не только помогают преступникам с низким уровнем технических навыков, но также делают операции зрелых и организованных злоумышленников более эффективными.

В 2001 г. европейские правоохранительные органы сообщили об увеличении предложения CaaS в темной Сети, среди которых партнерские программы по вымогательству кажутся наиболее заметными. Эти программы представляют собой эволюцию модели Ransomware-as-a-Service (программа-вымогатель как услуга, RaaS). В ней операторы делятся прибылью с партнерами, которые могут взломать целевую сеть, либо собирать всю информацию, необходимую для запуска атаки, либо самостоятельно развертывать вредоносное ПО.

Это расширило рынок продажи доступа к взломанной инфраструктуре и утечкам данных. Связанный с деятельностью операторов программ-вымогателей и мобильных вредоносных программ

доступ как услуга (AaaS) также пользуется большим спросом, поскольку он помогает как опытным командам — создателям вредоносных программ, так и преступникам низкого уровня, арендующим инструменты для доступа к корпоративным сетям.

Побочным продуктом роста многоуровневых схем вымогательства и широкомасштабных кампаний по воровству мобильной информации является приток личной информации на нелегальные рынки. Этот тип данных востребован широким кругом злоумышленников, поскольку он может значительно повысить вероятность успеха социальной инженерии, применяемой при любой форме атаки. В нынешнем виде пользователь часто остается самым слабым звеном в системе IT-безопасности. Это означает, что *социальная инженерия остается важным вектором для получения доступа к информационной системе* или, в случае мошенничества, к банковскому счету жертвы.

Широкое использование «серой» инфраструктуры. Помимо CaaS различные другие услуги, инструменты и технологии продолжают способствовать киберпреступности. Некоторые из них являются законными сферами, которые широко используются, но полезны и для достижения целей киберпреступников: безопасное общение, анонимность и многое другое.

Остальные услуги можно отнести к «серой» зоне. Такие службы часто находятся в странах с очень строгими законами о конфиденциальности. Они используются преступниками и рекламируются на криминальных форумах.

Услуги «серой» инфраструктуры включают в себя мошеннические обмены криптовалютой и виртуальные частные сети, которые обеспечивают безопасную деятельность преступников.

Самая известная особенность таких сервисов — надежное *сквозное шифрование*.

Европейские правоохранительные органы, однако, все больше сосредоточиваются на сервисах, которые не просто работают для обеспечения безопасности пользователей, но, скорее, оптимально защищают киберпреступников от захвата правоохранительными органами. Хотя не все пользователи таких услуг обязательно являются преступниками, уровень преступности, связанный с такими услугами, часто настолько высок, что национальные правоохранительные органы, обнаружив достаточно доказательств преступных

злоупотреблений, могут рассматривать их как преступные предприятия.

> В течение 2020 г. Европол вместе со своими партнерами скоординировал демонтаж различных сервисов, работающих в «серых» зонах. Например, были уничтожены две VPN, которые обеспечивали безопасность киберпреступников: DoubleVPN8 и Safe-Inet9. Ликвидация провайдеров зашифрованной связи (посредством криптофонов) привела к арестам сотен преступников и конфискации тонн запрещенных наркотиков, огнестрельного оружия и миллионов евро. Однако, что более важно, эти операции предоставили глобальным правоохранительным органам бесценную информацию о действиях преступников и их сетях.

Угроза мобильного вредоносного ПО. Мобильное вредоносное ПО уже долгое время представляет собой надвигающуюся угрозу в Европе, но так и не материализовалось в ожидаемой степени из-за отсутствия масштабируемости как устойчивой бизнес-модели. К сожалению, в последнее время киберпреступники совершили прорыв, и количество сообщений в правоохранительные органы о вредоносном ПО для мобильных устройств значительно увеличилось.

Число атак мобильного вредоносного ПО увеличивается по мере того, как все больше людей начинают использовать мобильные кошельки и платежные платформы.

В 2021 г. в 46% организаций хотя бы один сотрудник загрузил вредоносное мобильное приложение. Переход к удаленной работе почти для всех групп населения во всем мире во время пандемии COVID-19 привел к резкому увеличению площади мобильных атак, в результате чего 97% организаций столкнулись с мобильными угрозами, исходящими от нескольких векторов атак. Поскольку мобильные кошельки и мобильные платежные платформы используются все чаще, киберпреступления будут развиваться и адаптировать свои методы для использования растущей зависимости от мобильных устройств.

Ландшафт угроз для банковских троянов Android теперь включает новые тактики и методы кражи учетных данных. В ряде семейств вредоносных программ для мобильного банкинга реализованы новые возможности для совершения мошенничества пу-

тем манипулирования банковскими приложениями на устройстве пользователя с помощью модулей автоматизированной системы переводов (ATS) на базе Android Accessibility Service.

Банковские трояны, такие как Cerberus и TeaBot, также способны перехватывать текстовые сообщения, содержащие одноразовые коды доступа (OTP), отправленные финансовыми учреждениями и приложениями двухфакторной аутентификации (2FA), такими как Google Authenticator. Банковский вирус FluBot быстро распространяется. В настоящее время FluBot является одним из самых распространенных мобильных банковских троянов, сеющих хаос в Европе и США. FluBot позволяет осуществлять кражу учетных данных жертв (банковских, кредитных карт и криптокошельков). FluBot использует алгоритм генерации доменов (DGA) для подключения к своему серверу C2, генерируя список доменов, которые нужно попробовать, пока не найдется тот, с которым сможет связаться. Используя этот метод, злоумышленники могут быстро переключать домены, которые они используют для связи C2, когда они блокируются или отключаются. FluBot распространяется путем самораспространения, отправляя фишинговые текстовые сообщения с зараженного устройства контактам пользователя.

Возобновление денежно-мотивированных DDoS-атак. Правоохранительные органы сообщают о повторном появлении DDoS-атак, сопровождаемых требованиями выкупа, а также об увеличении массовых атак. Согласно докладу 2021 г., опубликованному Checkpoint, количество атак программ-вымогателей в мире выросло на 102% по сравнению с началом 2020 г., а наиболее целевыми секторами были здравоохранение и коммунальные услуги. В 2021 г. в мире каждая 61-я организация еженедельно подвергалась воздействию программ-вымогателей.

Киберпреступники нацелены на поставщиков интернет-услуг, финансовые учреждения, а также малый и средний бизнес. Обычно небольшая демонстрационная атака предшествует требованию выкупа. Злоумышленники, как правило, утверждают, что они связаны с APT-группировками[1], такими как Fancy Bear и Lazarus, чтобы запугать жертву и заставить ее заплатить выкуп. Имеются сообщения о последствиях несоблюдения требований, когда в одних

[1] Advansed persistent threat — постоянная угроза повышенной сложности.

случаях угроза крупномасштабной атаки не материализовалась, а в других, таких как атака на Новозеландскую фондовую биржу, злоумышленники выполнили свое обещание.

Киберпреступность с использованием программ-вымогателей будет продолжать расти, несмотря на усилия правоохранительных органов во всем мире. Злоумышленники будут нацелены на компании, которые могут позволить себе уплату выкупа, а атаки программ-вымогателей станут более изощренными. Хакеры будут все чаще использовать инструменты проникновения для настройки атак в реальном времени, а также для работы в сетях жертв. Инструменты проникновения являются движущей силой самых изощренных атак с использованием программ-вымогателей, имевших место в 2021 г. По мере роста популярности этого метода атаки злоумышленники будут использовать его для проведения атак с целью кражи данных и вымогательства.

Трансформация легальной торговли и криминальная сфера. Интернет-пространство изменило розничную торговлю. Цифровые торговые площадки сделали товары более доступными. Количество специализированных веб-сайтов и специализированных приложений быстро увеличилось, и они упростили доступ ко всем типам товаров и услуг.

Преступники используют и легальный, и теневой Интернет, где они предлагают все виды запрещенных товаров и большинство нелегальных услуг. Наличие и доступность безопасных онлайн-каналов привели к диверсификации платформ, используемых для незаконной торговли в Интернете. Распространение каналов связи с шифрованием данных и социальных сетей позволяет преступникам легко расширить аудиторию своих потенциальных клиентов.

Контрмеры преступников для обеспечения безопасности своих операций в сети Интернет. Преступники используют такие сервисы, как виртуальные частные сети (VPN), прокси-серверы и анонимные браузеры или «луковые» маршрутизаторы (Tor). Широко используются торговые площадки в социальных сетях, закрытые группы и мессенджеры, а также сервисы обмена зашифрованными сообщениями. Розничная торговля в Интернете обеспечивает прямой доступ к более широкому кругу потребителей. Это привело к резкому увеличению числа небольших посылок, отправляемых через почтовые или курьерские службы, для распростра-

нения запрещенных и нелегальных товаров. Из-за большого объема почтовых отправлений снижается вероятность обнаружения небольших партий товара.

Социальные сети дублируют рекламу на веб-сайтах и служат выделенными каналами для маркетинга или каналами связи для криминальных сетей.

Некоторые провайдеры предлагают *услуги безопасной связи с использованием модифицированных мобильных устройств.* У Европола существуют предположения, что отдельные провайдеры напрямую и преднамеренно обслуживают коммуникационные потребности преступников. Устройства, предлагаемые такими провайдерами, якобы гарантируют полную анонимность и не имеют таких функций, как камера, микрофон, GPS, порты USB, благодаря чему утрачивается любая связь между устройством или SIM-картой и пользователем. Зашифрованный интерфейс обычно скрыт и работает как часть двойной операционной системы. Подобные телефоны продаются через сети подпольных перекупщиков, а не через обычные точки розничных продаж.

Технологии шифрования широко используются как в законных, так и в незаконных целях. Шифрование обеспечивает конфиденциальность и целостность информации и защищает личные данные в процессе коммуникации. Сквозное шифрование стало стандартной функцией безопасности для многих каналов связи, включая приложения для обмена сообщениями и другие онлайн-платформы. Шифрование выгодно всем пользователям. К сожалению, это справедливо и в отношении преступников и криминальных сетей. Преступники уже много лет используют различные типы шифрования для защиты своих сообщений, передаваемых как через Интернет, так и традиционными способами, от контроля со стороны правоохранительных органов.

Финансовые потери предприятий, частных лиц и государственного сектора из-за выплат разработчикам программ-вымогателей. Ежегодно растут затраты на устранение последствий атак и расходы на усиление мер кибербезопасности.

Значительную угрозу представляют *кибератаки, направленные на жизненно важные объекты инфраструктуры,* — они могут повлечь за собой серьезные последствия, включая гибель людей. Быстро набирающая темп цифровизация общества и экономики постоянно создает новые возможности для злоумышленников, причастных к совершению киберпреступлений. Постоянный рост числа пользователей сети Интернет ведет к появлению новых слабых и уязвимых сторон и увеличивает число потенциальных целей для кибератак.

Хакерские программы постоянно совершенствуются и отличаются большим разнообразием — количество вариантов измеряется сотнями тысяч. Агентство ЕС по кибербезопасности (ENISA) каждый день сообщает об обнаружении 230 тыс. *новых разновидностей вредоносных программ.*

Быстрое распространение сложных цифровых технологий и широкое использование социальных сетей и средств для обмена зашифрованными сообщениями открывают для организаторов *незаконной перевозки мигрантов* возможности передавать информацию о своих услугах, согласовывать действия между собой и искать жертв, избегая обнаружения правоохранительными органами. Структуры, занимающиеся незаконной перевозкой мигрантов, используют криптовалюты, и в ближайшем будущем объем их использования может увеличиться. Незаконные перевозчики часто пользуются цифровыми услугами и инструментами, например социальными сетями и мобильными приложениями для вербовки, общения и совершения денежных переводов, встречи и передачи мигрантов, массовой мобилизации потоков мигрантов, обеспечения навигации на маршруте, обмена фото- и видеодокументов и билетов, а также отслеживания действий правоохранительных органов (по камерам видеонаблюдения и даже с дронов).

Жертвами организаторов договорных матчей все чаще становятся участники развивающегося *рынка киберспорта*. Существуют показатели, которые говорят о манипуляциях в киберспорте, среди них необычный всплеск ставок и необычно крупные суммы ставок перед самым началом матчей.

Во время пандемии COVID-19 спрос на цифровой контент, как легальный, так и нелегальный, резко возрос. Ожидается, что *распространение контента на физических носителях в ЕС полностью прекратится, поскольку его заменит более доступный цифровой контент.* Для оплаты доступа к пиратскому контенту будут широко использоваться виртуальные валюты. Число легальных способов доступа к развлечениям в Интернете увеличилось, и они ста-

ли дешевле для потребителей. Возможно, благодаря этому в будущем пиратский контент станет менее привлекательным.

Пиратское использование цифрового контента — это деятельность по нелегальному копированию и продаже цифрового контента, например музыки, книг, компьютерных программ и игр. Пиратство быстро эволюционирует одновременно с другими научно-техническими достижениями. *В настоящее время это почти исключительно цифровое преступление*, поскольку деятельность по распространению физических копий аудиовизуального контента почти полностью исчезла.

Кибератаки на цепи поставок. Злоумышленники пользуются отсутствием мониторинга в среде организации. В этих случаях можно использовать любой тип кибератак, например взлом данных и заражение вредоносным ПО.

> Хорошо известная атака киберпреступников на цепи поставок SolarWinds выделяется в 2021 г. своим масштабом и влиянием, но произошли и другие изощренные атаки на цепи поставок: на Codecov и на Kaseya. Kaseya предоставляет программное обеспечение для поставщиков управляемых услуг, а банда вымогателей REvil использовала компанию, чтобы заразить более тысячи клиентов с помощью программ-вымогателей. Группа потребовала выкуп в размере 70 млн долларов за предоставление ключей дешифрования для всех пострадавших клиентов.

Атаки на цепи поставок станут более частыми, и правительствам придется выработать меры борьбы с этими атаками и защиты сетей. Они также будут изучать возможности сотрудничества с частным сектором и в международном формате для выявления большего числа групп угроз, действующих в глобальном и региональном масштабах.

Кибернетические прокси-конфликты. Усовершенствованная инфраструктура и технологические возможности позволят террористическим группам и политическим активистам проводить более изощренные и широкомасштабные атаки. Кибератаки будут все чаще использоваться как прокси-конфликты для дестабилизации деятельности во всем мире.

Криптовалюта как мишень кибератак во всем мире. Когда деньги превращаются в чисто программное обеспечение, кибер-

безопасность, необходимая для защиты граждан от хакеров, крадущих и манипулирующих биткойнами и альткойнами, обязательно изменится неожиданным образом. В дальнейшем ожидается увеличение количества атак, связанных с криптовалютой.

Использование уязвимостей в микросервисах для запуска крупномасштабных атак. Переход к «облаку» и DevOps приведет к новой форме киберпреступности.

Поскольку микросервисы становятся ведущим методом разработки приложений, а архитектура микросервисов применяется поставщиками облачных услуг (CSP), злоумышленники используют уязвимости, обнаруженные в микросервисах, для запуска своих атак. Также можно ожидать появления крупномасштабных атак, нацеленных на CSP.

Технология Deepfake как оружие. Методы создания поддельных видео или аудио сейчас настолько развиты, что их можно использовать для создания целевого контента для манипулирования мнениями, ценами на акции или чем-то еще. Как и в случае других мобильных атак, основанных на социальной инженерии, результаты фишинговых атак могут варьироваться от мошенничества до более сложного шпионажа.

> Например, в ходе одной из самых серьезных фишинговых атак с использованием дипфейка управляющий банка в Объединенных Арабских Эмиратах стал жертвой мошенничества, совершенного злоумышленником. Хакеры использовали имитацию голоса искусственным интеллектом, чтобы обманом заставить менеджера банка перевести 35 млн долларов.

Злоумышленники будут использовать атаки социальной инженерии Deepfake для получения разрешений и доступа к конфиденциальным данным.

Возобновление кампаний дезинформации. Создание фейковых новостей, касающихся спорных вопросов, стало новым вектором атаки в последнее время. На протяжении 2021 г. распространялась дезинформация о пандемии COVID-19 и вакцинации. Черный рынок поддельных сертификатов о вакцинации расширился во всем мире, теперь подделки продаются из 29 стран. Поддельные сертификаты о вакцинации продавались по цене 100—120 долларов, и объем рекламы о продаже сертификатов за год увеличился в разы.

В дальнейшем кибергруппы продолжат использовать фейковые новостные кампании для совершения киберпреступлений с помощью различных фишинговых атак и мошенничества.

Кибератаки в сфере здравоохранения. Если здравоохранение не укрепит свою кибербезопасность, вскоре оно может оказаться в критическом состоянии. Такой вывод делает в своей статье на сайте ВЭФ С. Дюген, генеральный директор CyberPeace Institute. Исследование кибератак в сфере здравоохранения более чем в 30 странах, проведенное его институтом, показывает масштабы растущей угрозы.

Атаки программ-вымогателей доминируют среди участившихся угроз для поставщиков медицинских услуг. Трудно представить что-либо более циничное, чем блокирование информационных систем больницы с целью выкупа, но именно это и происходит все чаще и чаще.

Сектор здравоохранения — популярная мишень для киберпреступников. Недобросовестным злоумышленникам нужны данные, которые они могут продать или использовать для шантажа, но их действия ставят под угрозу жизнь.

CyberPeace Institute проанализировал данные о более чем 235 кибератаках (не считая утечки данных) на сектор здравоохранения в 33 странах с начала пандемии COVID-19. Хотя это лишь малая часть таких атак, но она является важным показателем растущей негативной тенденции и ее последствий для доступа к неотложной помощи.

Было украдено более 10 млн записей любого типа, включая номера социального страхования, медицинские карты пациентов, финансовые данные, результаты тестов на ВИЧ и личные данные медицинских доноров. В среднем во время одной атаки было взломано 155 тыс. записей, а при некоторых инцидентах сообщается о похищении более 3 млн записей.

Атаки программ-вымогателей, в ходе которых злоумышленники блокируют IT-системы и требуют оплаты за их разблокировку, оказывают прямое воздействие на людей. Услуги по уходу за пациентами особенно уязвимы. Исследователи обнаружили, что 15% атак программ-вымогателей приводили к перенаправлению пациентов в другие учреждения, 20% вызывали отмену приема у врача, получение некоторых услуг было прервано почти на четыре месяца.

В первой половине 2021 г. атаки программ-вымогателей происходили со скоростью четыре инцидента в неделю, и это только верхушка айсберга, поскольку во многих регионах отсутствует подобная статистика. Злоумышленники становятся более безжалостными, часто копируют данные и угрожают опубликовать их в Интернете, если они не получат дополнительную оплату.

Медицинские записи представляют собой цель с низким уровнем риска и высоким вознаграждением для киберпреступников — каждая запись может принести большую пользу на подпольном рынке, и вероятность того, что виновные будут пойманы, очень мала. Преступные группы действуют в самых разных юрисдикциях и регулярно обновляют свои методы.

1.4. ОПГ и кибермошенничество

Хотя ОПГ не пришлось заново изобретать свои методы работы, они продолжают их совершенствовать, делая их более целенаправленными и технически продвинутыми. Преступники продолжают получать значительную прибыль, а известные виды онлайн-мошенничества остаются эффективными.

COVID-19 продолжает оказывать значительное влияние на ситуацию с мошенничеством в мире в период пандемии.

Подделка компьютерной информации — противоправное совершенное намеренно действие, включающее ввод, изменение, удаление или подавление компьютерных данных, приводящее к получению недостоверных данных с намерением, чтобы они были восприняты как подлинные.

Эта категория киберпреступлений включает выдачу себя за законопослушных физических или юридических лиц в мошеннических целях. Здесь мошенничество можно рассматривать как искажение факта с целью убедить человека, группу людей, организацию предоставить преступнику что-то желаемое или ценное.

Компьютерное мошенничество — противоправное деяние, совершенное умышленно и приведшее к потере имущества другого лица посредством любого ввода, изменения, удаления или подавления компьютерных данных или любого вмешательства в функционирование компьютерной системы с мошенническим намерением получить, не имея на то права, экономическую выгоду для себя

или для другого лица. Эта категория киберпреступности включает использование ложной или вводящей в заблуждение информации для получения от жертвы того, что считается желательным или представляет ценность для преступника.

Банковское мошенничество — это общий термин, охватывающий способы незаконного получения денег, имущества или активов, принадлежащих финансовым учреждениям.

Платежное мошенничество — это разновидность банковского мошенничества. Мошенничество с платежами предполагает несанкционированное использование платежных данных физического лица для получения финансовой выгоды преступником.

Скимминг происходит, когда на терминале для карт установлено устройство для тайного сбора данных о кредитных, дебетовых или банковских картах пользователей. *Скиммер* — это тип устройства, предназначенного для тайного сбора такой информации. Один из типов скиммеров — это *скиммер для банкоматов.* Это устройство для чтения карт прикрепляется к той части банкомата, куда попадают кредитные карты.

Фишинговые преступники выдают себя за законные организации в сообщениях электронной почты. Их цель — войти в доверие к адресатам для того, чтобы те следовали инструкциям, предназначенным для побуждения жертвы неосознанно раскрыть личную и финансовую информацию; для доступа к вредоносным ссылкам или загрузки вредоносного ПО в системы жертвы. В результате злоумышленники получают несанкционированный доступ к компьютерным данным жертвы. Когда эта тактика нацелена на разных пользователей (а не на конкретную цель), это преступление обычно называют *фишингом.*

Схемы фишинга могут совершаться лицами, даже не имеющими технических навыков и способностей, потому что инструменты и ноу-хау легко доступны в Интернете (как часть модели «преступление как услуга»).

Мошенничество с предоплатой включает в себя требование к объекту заплатить деньги до получения чего-либо конкретного. Когда деньги получены преступником, жертве ничего не предоставляется взамен.

Романтическое (любовное) мошенничество. Исполнители любовных мошенничеств (или «ловли кошек») используют в своих целях потребность людей в общении. Эти мошенничества часто связаны с тем, что злоумышленники открывают поддельные профили на сайтах знакомств и платформах социальных сетей или используют чаты и другие форумы и веб-сайты для выявления жертв. Виновные в этом киберпреступлении используют тактику манипуляции, чтобы установить взаимопонимание с жертвами и завоевать их доверие. Во время этих мошенничеств преступник быстро заявляет, что влюбился в жертву, и постоянно осыпает ее знаками внимания, совершая соответствующие действия (например, пишет любовные письма, стихи и песни, отправляет небольшие подарки). После того как преступник добивается внимания и укрепляет доверие с жертвой, он пытается убедить ее предоставить деньги, товары или какую-либо услугу. История, обычно используемая в любовной афере, заключается в том, что преступник якобы попал в чрезвычайную ситуацию, требующую от жертвы отправки денег (например, неожиданная госпитализация или другое неотложное состояние, связанное со здоровьем). Преступник также может запросить средства для поездки, помощи в оплате неоплаченных счетов, покупки предметов, покупки или аренды дома или квартиры.

> Во Франции ОПГ находила своих потенциальных жертв на сайтах знакомств, воспользовавшись одиночеством и доверчивостью жертв. После того как преступники завоевывали доверие жертв, они просили их о помощи, включая деньги, для разрешения ситуации. После получения денег преступники обычно исчезали и больше не связывались со своими жертвами. В других случаях способ мошенничества был несколько иным: киберпреступники встречались со своими жертвами лично, пытаясь получить от них больше денег (тем самым совершая романтическую аферу как онлайн, так и лично).

Цель романтической аферы — заманить жертву в отношения (хотя и фальшивые, о чем жертве неизвестно). Преступник может притвориться, что имеет опыт, аналогичный опыту жертвы. Эта информация часто доступна в Интернете в профилях знакомств, учетных записях в социальных сетях и на других сайтах, содержащих информацию о жертве.

Иногда члены ОПГ похищают личную финансовую информацию жертвы и выдают себя за жертву, чтобы получить деньги и перевести средства с банковских счетов жертвы.

Мошенничество в Сети. Фишинг и социальная инженерия остаются основными векторами мошенничества с платежами, которые увеличиваются как в объеме, так и в изощренности.

Поскольку пандемия COVID-19 ограничивает поездки, переход к онлайн-покупкам увеличил возможности для мошенничества. Европейские правоохранительные органы сообщают об общем росте онлайн-мошенничества. Некоторые преступники используют приманки, связанные с COVID-19, такие как фишинг или продажа поддельной медицинской продукции. Другие стремятся использовать побочные эффекты пандемии. К ним относятся ослабление установленных процедур безопасности из-за того, что сотрудники работают из дома, и повсеместный переход к покупкам в Интернете. Распространение карантинных мер на всю Европу принесло с собой ряд новых возможностей электронной коммерции, которые часто оказывались мишенью для преступников. В частности, *мошенничество с доставкой* стало новым криминальным направлением на второй год пандемии. Преступники предлагают товары и получают оплату без доставки, обманывают интернет-магазины со слабыми мерами безопасности или используют службы доставки в качестве фишинговых приманок. Выдавая себя за службы доставки, преступники связываются с потенциальными жертвами посредством ссылок на фишинговые веб-сайты, якобы предлагающие информацию о доставке посылки, с целью получения учетных данных пользователя и данных платежной карты.

В последнее время значительно возросло количество попыток *фишинга*, связанных с COVID-19, в первую очередь с помощью телефона (*вишинг*) и текстовых сообщений (*смишинг*). В то время как испытанные и проверенные подходы социальной инженерии по-прежнему очень хорошо работают на преступников, фишинговые кампании продолжают развиваться. Скомпрометированная информация в результате утечки данных становится все более доступной. Преступники все чаще используют эту возможность, чтобы повысить свои шансы на успех путем создания целевых кампаний. Традиционно успешные преступления, такие как компрометация деловой электронной почты, вымогательство и другие виды мошенничества, связаны с доступностью личных данных потенциальных жертв. Поскольку эти данные могут иметь ключевое значение для повышения успешности преступной деятельности, это

привело к бесконечному циклу мошенничества, на котором процветает черный рынок скомпрометированной информации.

Вишинг и смишинг особенно выиграли от использования украденных данных в сочетании со *спуфингом*, когда с жертвами связываются, используя законно выглядящие идентификаторы вызывающего абонента или текстовые псевдонимы. Наряду с другими разработками мошенники часто сочетают традиционные попытки социальной инженерии с техническими компонентами, особенно в отношении жертв пожилого возраста. Например, все более частое использование троянов удаленного доступа (RAT) в вишинге основано на недостатке технических знаний у цели, что потенциально может привести к полному доступу к учетной записи и значительному финансовому ущербу.

Один из новых видов мошенничества — это *мошенничество с безопасным аккаунтом.* В этом виде мошенничества преступники с поддельными идентификаторами вызывающих абонентов беседуют со своими жертвами, притворяясь сотрудниками финансовых учреждений или полиции и информируя их о том, что им необходимо защитить свои деньги от преступников. Для этого жертве дают указание переводить свои средства на «безопасный счет», который на самом деле находится под контролем преступников и впоследствии используется «денежными мулами» для отмывания незаконных доходов.

Банковские фишинговые электронные письма — это мошеннические электронные письма, которые обманом заставляют получателей делиться своей личной, финансовой информацией или информацией о безопасности. Эти письма могут выглядеть идентично типам корреспонденции, которую отправляют реальные банки. Преступники копируют логотипы, макеты и тон реальных писем и просят вас скачать прикрепленный документ или перейти по ссылке. При этом указанные действия требуется сделать срочно.

В свете пандемии COVID-19 преступники использовали вишинг для получения доступа к банковским счетам жертв в странах, в которых медицинские услуги привязаны к идентификаторам мобильных банков. В этих случаях преступники связываются с гражданами по телефону и просят их сообщить сведения о себе, чтобы договориться о вакцинации или других медицинских услугах. Преступники использовали такой предлог, чтобы убедить

жертв предоставить документы, удостоверяющие личность, а потом получить доступ к их банковским счетам и обманом вынудить их перевести деньги преступникам.

Инвестиционное мошенничество стало наиболее распространенным видом мошенничества в последнее время.

В интернет-объявлениях жертв приглашают открывать онлайн-торговые портфели, заманивая выгодой при открытии. Однако вскоре, изъяв средства, мошенники исчезают. Также в качестве инвестиционных возможностей рекламируют несуществующие виртуальные валюты.

Поддельные инвестиционные веб-сайты особенно актуальны в этом контексте, поскольку преступники могут использовать недостаток знаний, а в некоторых юрисдикциях — нормативные препятствия, касающиеся доступа к биржам криптовалют. В то же время преступники продолжают совершенствовать этот вид мошенничества. Подлинно выглядящие рекламные кампании, незаконное использование знаменитостей и даже личные рекомендации через схемы онлайн-знакомств — все это помогает привлечь ничего не подозревающих жертв на эти поддельные платформы.

Кроме того, преступники становятся более профессиональными, создавая более легитимно выглядящие веб-сайты, используя программное обеспечение удаленного доступа для захвата учетных записей жертв и управляя сложными сетями «денежных мулов». Такое смешение различных методов работы — ключевая тенденция инвестиционного мошенничества.

С помощью подробных знаний о краже преступники часто могут обмануть своих жертв несколько раз: после кражи инвестиций преступники связываются с потерпевшими, выдавая себя за адвокатов или сотрудников правоохранительных органов, предлагая помощь в возврате средств.

Мошенничество, связанное с работой, включает рекламу вакансий и наем сотрудников, которые могут быть прикрытием для незаконной деятельности и операций. Незаконная деятельность, маскирующаяся под работу, может включать работу на работодателя, которая требует от работника: получать и отправлять товары из дома; получать и переводить денежные средства с личных банковских счетов на другие банковские счета; получать и обналичивать поддельные чеки; получать средства из различных источников, покупать товары или предоплаченные кредитные карты на эти деньги, а затем отправлять их по почте другим лицам; получать средства из различных источников, а затем переводить эти деньги другим лицам с помощью сервисов онлайн-платежей, денежных переводов, криптовалют.

Мошенничество на аукционах происходит, когда продавец выставляемого на аукцион предмета обманывает покупателей.

Мошенничество на аукционах может также включать недоставку предметов после того, как оплата была произведена, и доставку предметов нерекламируемых или более низкого качества, чем то, что рекламировалось. Этот тип мошенничества может заключаться в том, что продавцы намеренно завышают ставки, предлагая свои товары несколько раз, используя разные учетные записи.

Мошенничество с продажами в Интернете состоит в создании веб-сайтов, которые спроектированы так, чтобы выглядеть аналогично известным и популярным коммерческим веб-сайтам, и используются для продажи «товаров» — несуществующих, никогда не доставляемых, поддельных, но рекламируемых как подлинные, низкого качества.

> В Германии ОПГ управляла более чем 20 интернет-магазинами, которые предлагали кофе-машины или другие кухонные принадлежности. Веб-сайты были созданы по образцу популярных веб-сайтов электронной коммерции, в том числе веб-сайта известного многонационального предприятия онлайн-продаж. Клиенты должны были внести предоплату и получить автоматическое подтверждение заказа. Затем эти деньги переводились ОПГ.

Еще одним примером онлайн-мошенничества является *«ловушка подписки»* (потребители непреднамеренно берут платную подписку), когда веб-сайты рекламируют платные услуги, которые предлагаются бесплатно на других веб-сайтах. Такие услуги могут включать доступ к базам данных общедоступной информации, тесты (интеллект, любовь и секс и проч.), а также программное обеспечение.

Преступления, связанные с использованием личных данных. Такие преступления относятся к действиям, посредством ко-

торых устанавливается информация о личности, которая затем используется в незаконных целях.

Идентификационная информация считается онлайн-товаром. Личные, медицинские и финансовые данные покупаются, продаются и обмениваются онлайн за определенную плату в клирнете и даркнете. Тип идентификационной информации, которую ищут преступники, включает идентификационные номера (например, номера социального страхования), паспортные данные, национальную идентификационную информацию, информацию о водительских правах, данные медицинского страхования, информацию о финансовом счете, данные кредитной карты, данные дебетовой карты, сетевые учетные данные (например, информацию об учетной записи и пароли), адреса электронной почты, номера телефонов, IP-адреса и адреса управления доступом к мультимедиа.

Методы, используемые преступниками для получения нецифровой и связанной с цифровой идентификацией информации, включают: «ныряние» в цифровые мусорные контейнеры; кражу почты или перенаправление почты; кражу документов, удостоверяющих личность; использование общедоступной информации (например, публичных записей); скимминг; фишинг; фарминг (процедура скрытного перенаправления жертвы на ложный IP-адрес); установку вредоносного кода на компьютер или сервер, который автоматически направляет пользователя на мошеннический веб-сайт, имитирующий внешний вид законного веб-сайта; вредоносное ПО; взлом. Преступники могут также получить информацию, относящуюся к личности, путем простого поиска такой информации с использованием поисковых систем, платформ социальных сетей, веб-сайтов и общедоступных и частных баз данных в Интернете.

В США преступная организация Infraud Organization действовала в период с 2010-го по 2018 г. Незаконные действия, совершенные организацией, включали отмывание денег; незаконный оборот украденных средств идентификации; незаконный оборот, изготовление и использование поддельных идентификационных данных; кражу личных данных; незаконный оборот, производство и использование несанкционированных и поддельных устройств доступа; банковское мошенничество; мошенничество с использованием электронных средств. В организации насчитывалось более 10 тыс. членов по всему миру, прежде чем она была закрыта органами уголовного правосудия США в 2018 г.

Эта организация была хорошо известна тем, что продавала и рекламировала незаконные товары и услуги на онлайн-форуме, носящем название организации.

Роли лиц, которые были участниками этого преступного предприятия:

— администраторы. Они отвечали за долгосрочное стратегическое планирование предприятия и повседневные задачи управления, такие как определение обязанностей и уровней доступа всех членов, проверка потенциальных членов, принятие решения о том, какие люди могут присоединиться к организации, а также вознаграждение и наказание существующих членов;

— супермодераторы, которые отвечали за модерацию контента, проверяя контрабанду для продажи, редактируя и удаляя сообщения на основе обзоров, а также выступая посредниками в спорах между покупателями и продавцами;

— модераторы. У них были те же обязанности по модерированию контента, что и у супермодераторов, но было меньше полномочий и меньше привилегий;

— продавцы — физические лица, которые продавали или рекламировали на сайте незаконные товары и услуги;

— VIP-члены — давние, «выдающиеся» члены платформы;

— члены — все другие участники.

Основателями организации были два человека. Один выполнял функции администратора форума и управлял службой условного депонирования организации, которая использовалась для минимизации случаев мошенничества с поставщиками. Продавцы-мошенники были известны на сайте как «потрошители». Эти службы условного депонирования удерживали средства для покупки до тех пор, пока покупатель не получал купленные товары (в хорошем состоянии). Для контроля качества контрабанды, полученной в результате мошенничества и кражи личных данных, участники также предоставили отзывы и оценки поставщиков и их продуктов. Для безопасности участников этого преступного предприятия были приняты меры по защите форума и ограничению доступа к нему. Другой основатель установил правила, регулирующие поведение участников, которые соблюдались администраторами, модераторами и супермодераторами сайта. Участники, нарушившие

эти правила, наказывались блокировкой доступа на форум и другими санкциями. Все новые участники должны были пройти проверку перед тем, как получить доступ к форуму.

Один из основателей Infraud Organization признал себя виновным в заговоре с целью участия в преступной организации. 19 марта 2021 г. он был приговорен к 10 годам тюремного заключения. Другой основатель в настоящее время все еще на свободе.

Торговля фальсифицированной медицинской продукцией. Осуществляется как офлайн, так и онлайн. Такой оборот осуществляется через онлайн-торговые площадки, онлайн-аптеки, платформы электронной коммерции, социальные сети и другие платформы. Большинство интернет-аптек ведут бизнес незаконно и без соответствующих гарантий, в том числе не требуя рецепта, работают без лицензии (сертификата), не соблюдают национальные или международные правила в отношении аптек. Интернет-аптеки создают особые проблемы для следственных органов и органов судебного преследования, в том числе практические трудности при определении физического местонахождения.

Подделка. Она связана с незаконным изготовлением, продажей и распространением поддельной валюты, документов или продуктов. Традиционные ОПГ давно участвуют в незаконном обороте контрафактной продукции. Группы совершают эту форму торговли наряду с другими серьезными преступлениями, такими как незаконный оборот наркотиков, торговля людьми и отмывание денег. Средства, полученные от торговли контрафактной продукцией, часто подвергаются отмыванию и используются для разработки и продажи еще большего количества контрафактных товаров.

Поддельные продукты могут создаваться, представляться и продаваться так, чтобы выглядеть как товары, защищенные авторским правом, товарными знаками, они могут быть запатентованы в нарушение законов об интеллектуальной собственности.

Распространение поддельных денежных знаков также стало цифровым преступлением. В Интернете рекламируют и продают банкноты разных валют и номиналов, материалы и оборудование для нелегального изготовления, пособия, обучающие, как изготавливать поддельные деньги, и информацию об элементах защиты.

Мошенничество с безналичными платежами. Переход к безналичной экономике создает мощные стимулы для мошенников, специализирующихся на платежах. Киберпреступники стремятся взломать системы онлайн-платежей, интернет-банкинга и мобильного банкинга, онлайн-заявки на осуществление платежей, сервисы бесконтактной оплаты (как с использованием кредитной карты, так и без нее) и мобильные приложения. Рост использования мобильных устройств для осуществления финансовых операций и процедуры аутентификации сделал их мишенью для киберпреступников. Включает в себя все виды мошеннических действий, связанных с наиболее распространенными методами оплаты, включая платежи с использованием и без использования кредитной карты.

Мошенничество без предъявления карты (CNP), по-видимому, в значительной степени находится под контролем. В странах, где действительно увеличилось количество случаев CNP, преступники часто использовали обстоятельства пандемии COVID-19. Службы доставки еды, игровые платформы и другие платформы электронной коммерции были объектами мошенничества или использовались для кражи данных карт.

Переход от физических покупок к электронной коммерции привел к усилению внимания преступников к электронному скимингу. По мере того как через интернет-магазины совершается все больше и больше транзакций, наблюдается рост использования онлайн-скимминга с целью кражи данных карт. Хотя методы работы не изменились, преступники добавили в свои арсеналы ряд новых электронных скиммеров, в частности анализаторы JS. Когда во многих государствах — членах ЕС были введены жесткие ограничения в период пандемии, количество логических атак на банкоматы значительно сократилось. Такое развитие событий в основном связано с ограничениями COVID-19, не позволяющими преступникам путешествовать. Когда логические атаки на банкоматы прекратились, преступники с техническими способностями перешли на другие устройства для цифровых атак, в частности мобильные устройства. Однако снижение количества атак на банкоматы не было постоянной тенденцией. Как только запреты и ограничения на поездки были ослаблены, многие государства — члены ЕС начали сообщать о значительном росте преступности этого

типа. Банкоматы продолжают оставаться привлекательной мишенью для преступников. Многие старые модели банкоматов уязвимы для атак, поскольку в них не установлены последние обновления программного обеспечения.

В 2018 г. полиция Франции и ФБР США провели операцию, известную как «Операционный магазин карточек», для чего был создан тайный форум по кардингу (Carder Profit), который использовался для выявления киберпреступников, обменивающихся незаконными товарами и услугами, связанными с кардингом (использованием, продажей, совместным использованием или иным распространением украденных данных кредитной или дебетовой карты с целью совершения киберпреступления). В результате операции несколько человек были арестованы и преданы суду во Франции.

Подмена SIM-карт. Киберпреступники устанавливают контроль за использованием телефонного номера жертвы, по сути дезактивируя SIM-карту жертвы и перенося номер на SIM-карту, принадлежащую члену преступной сети. Как правило, преступники осуществляют подмену от имени поставщика телефонных услуг: либо через сотрудника компании, являющегося на самом деле коррумпированным инсайдером, либо с помощью методов социальной психологии.

Аферы с социальными пособиями. Они наносят существенный финансовый ущерб бюджету стран и могут лишить государственной поддержки тех, кто действительно нуждается в помощи. Мошенничество с социальными пособиями включает в себя аферы с медицинской страховкой, социальным пакетом, пособиями по безработице или пособиями низкооплачиваемым рабочим и беженцам. В рамках мошенничества с социальным демпингом криминальные структуры создают фиктивные компании, запрашивая выплаты социальных пособий несуществующим сотрудникам. В рамках другой разновидности такого мошенничества сотрудники продолжают работать, получая и пособие по безработице, и заработную плату по штатному расписанию работодателя.

Кредитное и ипотечное мошенничество. Это самая распространенная разновидность банковского мошенничества. Мошенники используют компании для получения ипотечных кредитов с помощью подтасованных сделок с недвижимостью. Мошенники нанимают бездомных или малоимущих лиц в качестве фиктивных заявителей на получение кредита в банках. В других случаях кредиты получают на основании поддельных паспортов. В рамках другого вида банковского мошенничества происходит захват счетов для проведения мошеннических сделок. Ипотечное мошенничество обычно связано с подделкой документов.

Мошенничество с субсидиями. Число случаев такого мошенничества с годами неуклонно возрастает. В рамках мошенничества с субсидиями преступники подают фальшивые заявления на получение грантов ЕС или на участие в тендерах. Как правило, такие заявления основываются на фальшивых декларациях, отчетах о ходе работ и счетах, которые используются для подтверждения государственных расходов или мошенническим образом полученных государственных тендеров и (или) субсидий.

Мошенничество с недоставкой. Это вариант мошенничества с платежным поручением или авансовым платежом. Такие мошенники рекламируют или продают несуществующие товары, используя фиктивный интернет-магазин. В первые месяцы пандемии COVID-19 мошенники пользовались высоким спросом и недостаточным объемом поставок средств индивидуальной защиты и наборов для самостоятельного проведения тестов. Число сайтов и аккаунтов социальных сетей, рекламирующих эти продукты в мошеннических целях, значительно выросло. Прибыли от этих мошеннических схем были немалыми, среди пострадавших оказалось много коммерческих и бюджетных организаций, например больниц или клиник, размещавших заказы на поставку на сумму в несколько миллионов евро.

Мошенничество с фальшивым счетом (мошенничество с платежным поручением или мошенничество со счетом-призраком). Мошенники требуют оплаты фальшивых счетов, выставленных потенциальным жертвам. Этот вид мошенничества основан на рекламных объявлениях на торговых интернет-сайтах.

Уклонение от уплаты пошлин на импорт товаров. Это отрицательно сказывается на финансовых интересах государств. Из-за демпингового импорта создается недобросовестная конкуренция с законопослушными предприятиями, и главнейшая составляющая в совершении мошенничества с НДС в каких бы то ни было целях — это технологии и цифровая инфраструктура. Крими-

нальные структуры используют технологии для сокрытия своей преступной деятельности, например удаленные серверы и хранилища данных, платформы цифровых и альтернативных платежей, VPN-услуги, зашифрованные сообщения и разные приложения интернет-мессенджеров для смартфонов.

Криминальные структуры теперь могут создавать и управлять компаниями с помощью только одного устройства, находящегося в любой стране, вести торговлю и передавать документацию по Интернету. Кроме того, сейчас есть бесплатное программное обеспечение для создания фальшивых счетов и банковских выписок. А благодаря новым способам перевода денег, таким как альтернативные банковские платформы, а также сервисам электронных банковских платежей вычислить злоумышленников стало еще сложнее.

Преступники принимают меры, чтобы не дать себя обнаружить, например, заменяют компании и их глав и используют новые технологии, чтобы оформлять компанию и скрывать ее владельца. Примерами гибкости и приспособляемости криминальных структур, действующих в данной области преступной деятельности, являются использование альтернативных банковских платформ в карусельных мошеннических схемах и попытки внедрить гарантии исходных рынков.

1.5. Вымогательство, шантаж и выкуп в Сети

Когда вымогательство осуществляется с помощью ИКТ, это называется *киберэксторсией.*

Шантаж — это форма вымогательства. Шантаж происходит, когда человек угрожает раскрыть компрометирующую информацию, предназначенную для того, чтобы поставить жертву в неловкое положение или причинить какую-либо другую форму вреда, если не будет выполнено требование.

Выкуп — это плата деньгами или имуществом преступнику, владеющему чем-то или кем-то ценным для жертвы, под угрозой причинения вреда.

Например, члены хакерской группы TDO были известны тем, что взламывали сайты организаций в сфере здравоохранения, развлечений, финансов, коммерции, недвижимости и транспорта, крали личную информацию из систем, которые они взломали, а затем добивались выкупа у жертв. Члены этой группы угрожали жертвам тем, что в случае неуплаты личная информация будет размещена в Интернете на хакерских форумах или публичных форумах или просочится к журналистам, что нанесет ущерб репутации компании или организации, которой принадлежат данные. Один из членов группы TDO, известный как Dark Overlord, был арестован и признал себя виновным в заговоре с целью совершения кражи личных данных и компьютерного мошенничества при отягчающих обстоятельствах. Он был приговорен к пяти годам тюремного заключения. Другие члены группы остаются на свободе.

Сексуальное вымогательство (или сексторсия) происходит, когда человек угрожает поделиться или иным образом распространить личную информацию или интимные изображения или видео, если жертва не предоставляет преступнику другие изображения или видео сексуального характера, не совершает половые акты на виду у преступника в Сети или не предоставляет преступнику деньги или товары.

Мошенничеством с выкупом занимаются преступники, которые притворяются представителями банков, кредиторов, юристов, правоохранительных органов или других государственных учреждений, требующими, чтобы непогашенная задолженность или другие вопросы были оперативно решены путем уплаты штрафа или другого сбора. Мошенничество с выкупом также может включать обзванивание жертв с ложным сообщением об аресте или задержании одного из родственников жертв с требованием денег за их освобождение.

Программы-вымогатели — это разновидность вредоносного ПО, которое заражает устройство пользователя и отправляет на устройство предупреждение о том, что, если жертва не совершит платеж, это повлечет за собой некоторые негативные последствия для владельца устройства. Этот тип вредоносного ПО также может быть разработан для блокировки доступа к данным, файлам или системам. Одной из форм программ-вымогателей является шифровальщик-вымогатель, троянский конь, предназначенный для шифрования данных в системе жертвы и вымогательства денег у жертвы для раскрытия информации.

Операторы вредоносных программ, особенно те, которые связаны с партнерскими программами вымогателей, улучшили свои ме-

тоды атак и функциональные возможности вредоносных программ. Мобильные банковские трояны совершили прорыв благодаря растущему числу пользователей, предпочитающих вести свою финансовую деятельность через мобильные устройства.

Программы-вымогатели продолжают доминировать и распространяться.

Несмотря на то что мир радикально изменился в последнее время, одна константа осталась неизменной — это угроза, которую программы-вымогатели представляют для нашей финансовой, общественной и даже физической безопасности. Большинство респондентов из правоохранительных органов отметили, что за отчетный период увеличилось количество сообщений о программах-вымогателях. Тенденции сосредоточения внимания на крупных корпорациях и государственных учреждениях, использования уязвимостей в цифровой цепи поставок и многоуровневого вымогательства, которые мы наблюдали в недавнем прошлом, усилились и стали более заметными, что свидетельствует о возросшей сложности и зрелости задействованных партнерских программ-вымогателей.

Распределенные атаки типа «отказ в обслуживании» (DDoS) с целью выкупа могут вернуться из-за растущей зависимости от онлайн-сервисов.

Киберпреступники продолжают двигаться к более продуманному выбору целей, и растет число партнерских программ по вымогательству, предполагающих сотрудничество с хакерами и другими разработчиками вредоносных программ.

Эти тенденции были отмечены в предыдущем IOCTA, но переход произошел быстрее, чем многие могли ожидать, за 2021 г. обнаружились многочисленные крупномасштабные вторжения.

Преступники продолжают действовать все более безжалостно и методично. Европол писал о росте числа бригад вымогателей, использующих методы двойного вымогательства путем извлечения данных жертв и угроз их публикации.

Многие из самых известных партнерских программ по вымогательству разворачивают DDoS-атаки против своих жертв, чтобы заставить их выполнить требование выкупа. Эти методы работы становятся все более популярными среди преступников, занимающихся мошенничеством с инвестициями, что, по мнению

правоохранительных органов Европы, является одной из основных угроз. Те, кто организует эти схемы, создают местные центры обработки вызовов, чтобы повысить доверие к ним среди пострадавших, говорящих на разных языках, а также перенацеливать своих «клиентов». Как только человек осознает, что его инвестиции были украдены, мошенники снова связываются с ним под предлогом, что представляют юридические фирмы или правоохранительные органы, предлагая помочь вернуть их средства.

В свете этих событий рынок криминальных товаров и услуг переживает бум. Личная информация и учетные данные пользуются большим спросом, поскольку они играют важную роль в повышении успешности всех приемов социальной инженерии. К сожалению, рынок личной информации процветает, поскольку программы-вымогатели и мобильные кражи информации производят множество материалов для продажи в качестве побочного продукта первичной атаки.

Программы-вымогатели эволюционировали, из нацеленных на отдельных пользователей ИКТ они стали более целенаправленными. Злоумышленники переходят к управляемым человеком программам-вымогателям, нацеленным на частные компании, секторы здравоохранения и образования, критически важную инфраструктуру и государственные учреждения.

Изменение парадигмы атаки указывает на то, что операторы программ-вымогателей выбирают цели на основе их финансовых возможностей, соответствующих более высоким требованиям к выкупу, и их потребности как можно быстрее возобновить свои операции.

Уделять больше времени крупным корпорациям и государственным учреждениям — это эффективный подход для киберпреступников с точки зрения окупаемости инвестиций. Однако злоумышленники начали рассматривать внимание правоохранительных органов, привлекаемое к их деятельности, как важный критерий для внутреннего анализа затрат и выгод.

С начала пандемии киберпреступники воспользовались тем фактом, что большинству компаний пришлось хотя бы частично прибегнуть к дистанционной работе. Это означало, что IT-безопасность стала контролироваться хуже, а общее количество уязвимостей и поверхности атаки увеличились.

Злоумышленники продолжали проникать в сети организаций через подключения по протоколу удаленного рабочего стола (RDP) и эксплуатировать уязвимости в службах VPN.

Преступники осознали, насколько велик потенциал компрометации цифровых цепей поставок — организациям необходимо предоставить доступ к сети дистрибьюторам обновлений, что делает этих сторонних поставщиков услуг идеальной целью. После проникновения в клиентскую сеть поставщика программного обеспечения операторы программ-вымогателей могут выбрать наиболее подходящие цели, далее проходят через свою сеть под видом законных пользователей, а затем разворачивают свой вредоносный код в наиболее подходящий момент. Кроме того, IT-инфраструктуры чрезвычайно взаимосвязаны, поэтому успешное вторжение не только подвергает риску клиентов одной компании, но потенциально также открывает двери для компрометации других поставщиков услуг, обеспечивая еще большую масштабируемость атаки.

Атаки программ-вымогателей стали более изощренными, поскольку преступники проводят больше времени внутри Сети, исследуя цель, чтобы еще больше скомпрометировать инфраструктуру и получить больше данных.

Злоумышленники начали более широко использовать бесфайловые вредоносные программы (с использованием собственных средств системы для выполнения кибератак), чтобы избежать распространенных методов обнаружения, которые сканируют вложения вредоносных файлов или создание новых файлов. Бесфайловые атаки программ-вымогателей используют собственные языки сценариев для записи вредоносного кода непосредственно в память целевой системы или захватывают встроенные инструменты для шифрования файлов.

Команды программ-вымогателей начали использовать службы передачи голоса по интернет-протоколу (VoIP), чтобы, например, вызывать журналистов, клиентов организации и деловых партнеров для дальнейшего продолжения вымогательства.

В некоторых случаях операторы программ-вымогателей угрожают своим жертвам DDoS-атаками и публикацией личной информации своих сотрудников, если они не выполнят требование выкупа.

Есть сведения о резком росте количества выплаченных выкупов (увеличение более чем на 300%) в период с 2019-го по 2020 г. из-за большего времени, затрачиваемого на выполнение атак, и многоуровневых методов вымогательства.

> В январе 2021 г. правоохранительные и судебные органы по всему миру отключили ботнет Emotet. Emotet был установлен на компьютеры жертв через электронные письма, содержащие вредоносную ссылку или зараженный документ. Если жертвы открывали вложение или ссылку, вредоносное ПО устанавливалось. Компьютер становился уязвимым и предлагался в аренду другим преступникам для установки других типов вредоносных программ. Как работал Emotet? Заманивание жертв, установка инфекции Trickbot. QakBot и Ryuk были среди семейств вредоносных программ, которые использовали Emotet для проникновения в машину. Emotet открыл двери для троянских программ-вымогателей, похитителей информации об известных транзакциях на общую сумму более 400 млн долларов США. Кроме того, средняя сумма выплачиваемого выкупа увеличилась со 115 123 долларов США в 2019 г. до 312 493 долларов США в 2020 г. (увеличение более чем на 170%).

Все дополнительное время и усилия, затрачиваемые на атаки программ-вымогателей для получения более крупных выплат, обеспечиваются постоянным развитием и специализацией экосистемы криминальных структур (модель «преступление как услуга»). За 2021 г. был отмечен рост партнерских усилий по программам-вымогателям независимо от того, продаются ли они публично широкому кругу потенциальных пользователей или предлагаются частным образом небольшой группе хакеров.

Общедоступные партнерские программы-вымогатели — не совсем новое явление, поскольку субъекты, взламывающие систему жертвы и затем платящие оператору за использование своего вредоносного ПО, уже довольно давно наблюдаются в экосистеме киберпреступников. Больше поводов для беспокойства вызывает рост частных партнерских программ, которыми обычно управляют более известные преступные группы вымогателей. Эти злоумышленники ищут разработчиков и хакеров, чтобы улучшить функциональность вредоносного ПО или получить

доступ к инфраструктуре важных целей. Команды программ-вымогателей также сотрудничают с другими разработчиками вредоносных программ.

1.6. Сексуальное насилие над детьми в Интернете

Материалы о сексуальном насилии над детьми и материалы о сексуальной эксплуатации детей создаются и распространяются через веб-сайты, группы новостей в Интернете, программное обеспечение для веб-конференций, платформы социальных сетей, незашифрованные и зашифрованные коммуникационные приложения и другие онлайн-платформы. Эти материалы также распространяются с помощью текстовых сообщений, обмена мгновенными сообщениями, сообщениями электронной почты, чатов, досок объявлений и одноранговых сетей обмена файлами. Виновные в сексуальном насилии над детьми и сексуальной эксплуатации детей в Интернете могут быть членами крупных онлайн-сообществ или небольших сообществ, где материалы о сексуальном насилии над детьми пересылаются напрямую между преступниками с использованием различных приложений, таких как платформы для обмена зашифрованными сообщениями.

Обмен информацией в этих сообществах строго контролируется правилами присоединения к платформе и кодексами поведения. Правила соблюдаются модераторами и администраторами сайтов, а участники сайтов должны соблюдать официальные правила присоединения и кодексы поведения, чтобы оставаться активными участниками на сайтах. Активное участие в форумах создает репутацию человека и может повысить его положение или звание в сообществе. Активное участие в этих форумах связано с рекламой, размещением, распространением материалов о сексуальном насилии над детьми и материалов о сексуальной эксплуатации детей. Чтобы сохранить доступ к сайтам или получить доступ к большему количеству материалов о сексуальном насилии над детьми и сексуальной эксплуатации детей на сайте, участники должны постоянно публиковать такие материалы. Неспособность внести свой вклад в сайт приведет к аннулированию прав и удалению с сайта.

Способы вовлечения детей в сексуальную эксплуатацию в Сети:

— установление контакта с ребенком, который можно охарактеризовать как средство, с помощью которого взрослый «подружился» с ребенком с намерением изнасиловать его. Установление контакта с детьми может происходить как онлайн, так и офлайн. Исследования показывают, что жертвами этого преступления в основном являются девочки, тогда как мужчины — преимущественно исполнители этого преступления.

Процессы установления контакта различаются. Однако важными элементами являются: отбор жертвы, основанный на привлекательности, легкости доступа и уязвимости жертвы; контакт с жертвой; установление взаимопонимания и формирование дружбы между преступником и жертвой;

— опросы. В чате проводятся текущие опросы участников о привлекательности несовершеннолетних, или участники голосуют за то, какой тип одежды несовершеннолетний должен снять или какой тип полового акта следует совершить несовершеннолетнему;

— соревнования. Несовершеннолетние соревнуются друг с другом в попытке получить вознаграждение (т. е. они получают баллы за участие в определенном сексуальном поведении и половых актах и переходят на более высокий уровень на основе баллов);

— предложения заблокировать веб-камеры. Чтобы несовершеннолетние стали более раскованными, член ОПГ, которому жертва доверяет (называемый «обработчиком»), утверждает, что он может заблокировать веб-камеру жертвы и запретить другим участникам чата просматривать жертву;

— петли. Это предварительно записанные видео, на которых другие несовершеннолетние разговаривают или участвуют в сексуальном поведении или половых актах, воспроизводимые так, как происходящее в реальном времени, чтобы манипулировать несовершеннолетним, заставляя его участвовать в аналогичном поведении.

Сексуальное насилие над детьми может совершаться в прямом эфире. Участники прямой трансляции могут быть пассивными или активными зрителями. Пассивные зрители платят за просмотр, в то время как активные зрители платят за то, чтобы сыграть свою роль в сексуальном насилии над детьми, сообщая, какие сексуальные действия они хотят видеть в исполнении насильников, ребенка или тех, кто занимается с ним (активные зрители совершают то, что известно как «сексуальное насилие над детьми по заказу»).

Основные тенденции и угрозы, связанные с сексуальной эксплуатацией детей в Интернете, в течение определенного периода оставались относительно стабильными. На производство и распространение материалов о сексуальном насилии над детьми (CSAM) повлияло растущее бесконтрольное присутствие детей в Интернете. Распространение приложений для обмена зашифрованными сообщениями и платформ социальных сетей влияет на методы обработки и распространения CSAM среди правонарушителей.

Производство и распространение CSAM в Интернете стало серьезной проблемой с момента появления Интернета. Правоохранительные органы и некоммерческие организации, занимающиеся защитой детей, ежегодно обнаруживают огромное количество таких материалов. Во многих случаях преступники производят CSAM в домашней среде жертвы, чаще всего создаваемой теми, кто находится в кругу доверия ребенка.

Дети выходят в Интернет без присмотра в очень раннем возрасте и проводят долгие часы за электронными устройствами. Это подвергает их серьезным угрозам. Пандемия COVID-19 оказала значительное влияние на присутствие детей в Интернете. Национальные ограничения вынудили к дистанционному и виртуальному обучению, в то время как невозможность участия в социальной деятельности привела к тому, что значительно больше времени проводилось в онлайн-играх и на платформах социальных сетей.

Кроме того, более либеральное отношение к публичному обсуждению сексуального поведения в Интернете меняет отношение молодых людей к обмену откровенным контентом друг с другом. Эти социальные изменения предоставили правонарушителям более широкую группу потенциальных жертв.

В 2020 г. правоохранительные органы сообщали о резком росте обнаружения самогенерируемых материалов, которыми обмениваются в социальных сетях, в том числе с изображением детей младшего возраста. Неправительственные организации, занимавшиеся обнаружением и удалением онлайн-сообщений CSAM, сообщают, что почти две трети подтвержденных отчетов содержали самодельные материалы, часто созданные в собственной спальне жертвы. Злоумышленники используют уязвимости, чтобы войти в контакт и завоевать доверие несовершеннолетних в Интернете,

прежде чем приступить к злоупотреблениям, ведущим к самопроизвольной деятельности жертв.

Правоохранительные органы сообщают о пике случаев онлайн-груминга (общения взрослого человека с несовершеннолетним) за 2021 г., особенно в социальных сетях и на игровых платформах. В других случаях несовершеннолетние вступают в сексуальные отношения в Сети со взрослыми, которые завоевывают их доверие, выдавая себя за их сверстников. Преступники, скрываясь за вымышленными личностями, часто получают самодельные материалы с помощью манипуляций или шантажа. Некоторые исследования указывают на создание подростками сексуальных образов и обмен ими как на исследование своей сексуальности. Несовершеннолетние также создают материалы для финансовой выгоды и для повышения своего онлайн-статуса на определенных платформах, собирая лайки и другие индикаторы одобрения.

Некоторые правонарушители переходят из Сети в офлайн. В отдельных случаях злоумышленники убедили жертв встретиться в реальной жизни, превратив онлайн-насилие в физическое, которое также может продолжаться в течение долгого времени посредством принуждения или вымогательства.

Количество случаев жестокого обращения с детьми на расстоянии (LDCA) продолжает увеличиваться.

Ограничения на поездки и контакты, вызванные пандемией COVID-19, вероятно, повлияли на угрозу LDCA, что сделало их жизнеспособной альтернативой для тех, кто обычно является транснациональными преступниками в отношении сексуального насилия над детьми. LDCA может быть дополнительным источником производства CSAM. Некоторые правонарушители записывают или захватывают жертв, совершающих в их интересах сексуальные действия в прямом эфире, без ведома жертв. Правоохранительные органы наблюдали за обменом новыми «закрытыми» материалами на форумах Dark Web.

CSAM обычно хранится в Сети или локально на защищенных паролем дисках. Преступники часто используют сквозные зашифрованные каналы связи, платформы социальных сетей и доски объявлений для распространения незаконного контента. Частные группы, посвященные обмену CSAM, продолжают расти в приложениях для обмена сообщениями. Одноранговые (P2P) сети обмена

файлами остаются важным каналом для обмена CSAM от пользователя к пользователю или в небольших группах. Некоторые страны сообщили о значительном общем увеличении использования распределительных сетей P2P. Эта тенденция согласуется с пиком, зарегистрированным на ранних стадиях пандемии COVID-19 и позже подтвержденным при сравнении данных за 2019 и 2020 гг. Однако в отчете IOCTA 2020 г. сообщалось о снижении активности P2P.

Несмотря на успешные действия правоохранительных органов по закрытию платформ, ориентированных на сексуальное насилие над детьми, группы, способствующие обмену CSAM в Dark Web, продолжают расти и представляют собой постоянную угрозу. Преступники часто обмениваются незаконным контентом в этих группах через прямые ссылки на хосты изображений в клирнете и даркнете, где хранится CSAM. В некоторых случаях они также используют сайты киберблокировщиков, где пользователи платят поставщикам контента за каждую регистрацию и последующую загрузку своего контента.

Форумы с материалами о сексуальном насилии над детьми хорошо структурированы, а посетители организованы иерархически, согласно их ролям. Посетители берут на себя роли в зависимости от их вклада в сообщество и могут быть администраторами, модераторами или пользователями. В некоторых случаях посетители берут на себя роль модераторов на нескольких платформах, облегчая распространение CSAM среди более широкой аудитории. Использование этих специализированных платформ не ограничивается распространением материалов, но открывает форум для обмена мнениями среди единомышленников, где правонарушители могут поделиться опытом, методами совершения злоупотреблений и успешными контрмерами для уклонения от обнаружения или предотвращения обнаружения. Эти сети хорошо структурированы, управляемы и достаточно сплочены. Новые посетители должны завоевать доверие сообщества, чтобы быть принятыми в группу, например, путем участия в недавно созданном или опубликованном CSAM. Отсутствие в Сети одного из участников может вызвать беспокойство в сообществе.

За исключением LDCA, преступления, связанные с сексуальным насилием над детьми, обычно не совершаются с целью получения финансовой выгоды. Однако монетизация CSAM представляет собой растущую угрозу. Годовой доход сайтов CSAM, по оценкам, увеличился более чем в три раза в период с 2017-го по 2020 г. Криптовалюты являются предпочтительной валютой для этих типов транзакций. В некоторых случаях правонарушители платят несовершеннолетним напрямую за обмен собственноручно созданным контентом. Правоохранительные органы заметили изменения в использовании онлайн-платформ, которые должны использоваться взрослыми только для обмена откровенным контентом для взрослых. Некоторые из этих платформ не могут предотвратить доступ несовершеннолетних, которые регистрируются с поддельной идентификацией и появляются в откровенных видео.

Только Европол в настоящее время располагает более чем 40 млн изображений, иллюстрирующих сексуальную эксплуатацию несовершеннолетних в разных странах мира.

> Платформа на Dark Web, известная как Boystown, была заблокирована международной целевой группой, созданной федеральной уголовной полицией Германии. В нее входили Европол и правоохранительные органы из Австралии, Канады, Нидерландов, Швеции и США. Этот сайт был посвящен сексуальному насилию над детьми, и на момент его закрытия у него было 400 тыс. зарегистрированных пользователей. В то же время были заблокированы несколько других чатов в Dark Web, используемых несовершеннолетними преступниками, совершившими сексуальные преступления.
>
> Онлайн-сообщества несовершеннолетних правонарушителей в Dark Web демонстрируют значительную устойчивость в ответ на действия правоохранительных органов, направленные на них. Их реакция включает возрождение старых сообществ, создание новых сообществ и принятие решительных мер по их организации и управлению.

Европейская комиссия работает над предложением о создании *центра ЕС по предотвращению и противодействию сексуальному насилию над детьми.* Его цель — обеспечить эффективный и скоординированный подход к противодействию сексуальному насилию над детьми в ЕС. Он будет охватывать профилактику и поддержку пострадавших. Центральная роль Европола, как это предусмотрено Комиссией ЕС, в предлагаемом центре ЕС по предотвращению

сексуального насилия над детьми и борьбе с ним будет гарантировать, что он продолжит предоставлять высококачественные услуги государствам — членам ЕС и партнерам, заключившим рабочие соглашения. Подход Европола по противодействию сексуальному насилию над детьми в Интернете ориентирован на жертв, о чем свидетельствуют деятельность Целевой группы по идентификации жертв и такие инициативы, как «Отследить объект — спасение ребенка», превентивные инициативы (например, #SayNo).

1.7. ОПГ и Dark Web

Пользователи Dark Web все чаще используют Wickr и Telegram в качестве каналов связи.

Пользователи Dark Web используют анонимные криптовалюты, такие как Monero, и службы обмена.

Пользователи полагаются на все более сложную операционную безопасность, быстро мигрируя на другие (беспользовательские) рынки.

«Серая» инфраструктура все больше способствует процветанию пользователей Dark Web.

Последние годы показали множество успешных международных совместных попыток уничтожения рынков Dark Web. Тем не менее некоторые продавцы и рынки продолжают существовать. Продавцы и другие пользователи рынков Dark Web, в том числе в сфере сексуальной эксплуатации детей, просто мигрируют на новую платформу после успешного закрытия старой на Dark Web правоохранительными органами.

Присутствие групп программ-вымогателей на выделенных скрытых сервисах в Dark Web, предлагающих свои вредоносные программы как услугу, увеличилось.

Оружие все чаще продается в зашифрованных приложениях, таких как Telegram и Wickr, но на торговых площадках Dark Web продается не намного меньше.

Европол оказал помощь в аресте гражданина Италии, подозреваемого в найме киллера в Dark Web. О нескольких подобных случаях сообщалось в СМИ.

Например, в Нидерландах человека приговорили к восьми годам тюремного заключения за несколько попыток заказать убийство с помощью платформ в Dark Web и зашифрованных приложений чата. Кроме того, оружие продавалось на торговой площадке Dark Web, закрытой в мае 2021 г. французскими властями. В сентябре 2020 г. в Испании был демонтирован нелегальный цех по печати трехмерного оружия, что свидетельствует о новом методе работы. Подозреваемый скачал из даркнета шаблоны для печати оружия. Во время одного из обысков дома в рамках совместной операции Налогового управления Испании и Национальной полиции сотрудники правоохранительных органов обнаружили различные 3D-принтеры, на одном из которых производилась печать небольшого огнестрельного оружия.

Правоохранительные органы ЕС выявили угрозу фрагментации Dark Web, которая проявляется в различных способах работы. Правоохранительные органы ЕС сообщили о дальнейшем увеличении числа магазинов с одним продавцом и небольших рынков на Tor и указали, что фрагментация также заметна в криминальных сетях, поскольку они, как правило, используют различные учетные записи на разнообразных торговых площадках. Кроме того, например, увеличилось использование зашифрованных коммуникационных платформ за пределами торговых площадок Dark Web для продажи незаконных товаров и услуг. В частности, правоохранительные органы несколько раз упоминали Wickr и Telegram. Например, в одной стране 70% поставщиков, которые, по-видимому, работают из этой страны, указали в своем профиле рынка Dark Web имя пользователя Wickr, а 20% указали контактную информацию Telegram. Все более широкое использование преступниками платформ с надежным шифрованием, которые в основном используются в законных целях, создает проблему для правоохранительных органов. Это также показывает, что исследователям Dark Web необходимо обратить внимание на другие платформы. Так, по мнению правоохранительных органов, система Televend автоматизирует часть процесса продажи и покупки, но также включает меньше механизмов безопасности, что повышает вероятность мошенничества пользователей.

Немецкие правоохранительные органы уже провели успешную операцию, отключив девять групп Telegram, в которых продавались нелегальные товары и услуги, что свидетельствует: это но-

вое явление также не исключает вмешательства правоохранительных органов.

Биткойн до сих пор оставался предпочтительной криптовалютой для пользователей Dark Web. Однако преступное использование конфиденциальной монеты Monero на торговых площадках Dark Web еще больше увеличилось. Monero становится самой популярной монетой конфиденциальности в Dark Web.

Использование обменников относится к тенденции применения более сложных методов отмывания денег. На заре создания торговых площадок Dark Web поставщики часто просто переводили криптовалюту напрямую с торговой площадки на биржу. Тем не менее за последние несколько лет популярность приобрели многие различные методы обфускации (запутывания кода), такие как микшеры, CoinJoin, своппинг, крипто-дебетовые карты, биткойн-банкоматы, местная торговля и многое другое.

1.8. Глобальные тренды

Развитие технологий идет буквально с космической скоростью. Помимо благих целей любая технология четвертой промышленной революции может быть использована в деструктивных целях.

В 2020 г. компания RAND Europe провела анализ тенденций развития будущих технологий для определения тех, которые могут быть использованы для совершения киберпреступлений.

Растущая доступность более мощных, простых в использовании и менее дорогих технологий, вероятно, будет еще больше стимулировать киберпреступность за счет увеличения круга лиц, заинтересованных в быстром получении финансовой выгоды.

Разработка новых сложных технологических решений и возможностей может позволить «специалистам» в области киберпреступности, организованным группам осуществлять сложные атаки и действия, приводящие к более высоким доходам от преступной деятельности и, возможно, к тяжким последствиям для отдельных лиц и организаций.

Повышенная скорость и увеличение зоны покрытия связи будут способствовать еще большему снижению влияния расстояний на телекоммуникации, что будет использовано киберпреступниками.

Искусственный интеллект (AI)/машинное обучение (ML) могут сделать киберпреступления более эффективными и масштабируемыми. Достижения в области AI/ML усложнят отслеживание и атрибуцию преступных и злонамеренных действий. Это будет способствовать повышению привлекательности киберпреступности, усилению нагрузки на правоохранительные органы.

Автономные устройства и системы могут проникнуть в пространства, которые ранее были недоступны для людей, использоваться для совершения замаскированных преступных действий, разработки новых методов преступной деятельности или проведения крупномасштабных и автоматизированных атак.

Развитие и повсеместное распространение вычислительной техники и технологий хранения данных может облегчить кражу данных, хранение и распространение незаконных данных.

Развитие инфраструктуры электросвязи может быть использовано для повышения анонимности, скорости преступной деятельности, в частности кражи личных и конфиденциальных данных. Инфраструктура электросвязи также может быть использована преступниками для крупномасштабных сбоев.

Растущие объемы данных, собираемых устройствами Интернета вещей (IoT), могут стать уязвимыми для краж, коррупции, вымогательства. Устройства IoT также могут увеличить поверхность атаки для киберпреступлений и внести новые уязвимости в сложные IT-системы.

Технологии улучшения конфиденциальности пользовательского интерфейса (ПЭТ) злоумышленники будут использовать для анонимной и тайной незаконной деятельности, что затрудняет обнаружение, мониторинг и расследование преступной деятельности. ПЭТ также могут быть целью злоумышленников для доступа к конфиденциальной или частной информации.

Блокчейном пользовательского интерфейса и технологией распределенного реестра (DLT) можно будет манипулировать в злонамеренных целях, например для взлома консенсуса. DLT также можно использовать для хранения разрушительного или неприемлемого контента, что затрудняет его удаление.

Разработка и внедрение устройств и продуктов с низкими стандартами безопасности и гарантиями расширят существующий ландшафт уязвимостей, которые могут быть использованы злоумышленниками.

Разработки в области вычислительной техники и технологий хранения данных в сочетании с увеличением количества устройств будут способствовать увеличению количества возможных преступных и злонамеренных действий, включая разработку новых методов преступной деятельности.

Подрыв доверия к технологиям и связанным с ними продуктам и услугам приведет к увеличению объема и воздействия любых связанных с ними уязвимостей и сбоев. Эти уязвимости также могут иметь каскадные эффекты, которые трудно предсказать или смягчить во все более сложных и нелинейных системах. В этом контексте потенциально латентные случаи преступлений могут привести к гораздо более широким последствиям из-за ранее непредвиденных связей и встроенных взаимозависимостей.

В компании FortiGuard (один из мировых лидеров в области интегрированных и автоматизированных решений в сфере информационной безопасности) в 2021 г. оценены *стратегии, которые киберпреступники будут использовать в ближайшие годы*.

За последние несколько лет в отчетах компании были затронуты такие вопросы, как эволюция программ-вымогателей, риски расширения цифрового присутствия бизнеса и нацеливание на конвергентные технологии, особенно те, которые являются частью интеллектуальных систем, таких как «умные» здания, города и критически важные инфраструктуры. Компания также рассмотрела эволюцию морфического вредоносного ПО, серьезный потенциал атак на основе роя, а также использование искусственного интеллекта и машинного обучения в качестве кибероружия. Некоторые из этих технологий уже осуществлены, а другие успешно продвигаются.

В последние годы традиционный периметр Сети был заменен несколькими периферийными средами, WAN[1], мультиоблачными средами, центрами обработки данных, удаленным работником, Интернетом вещей (IoT) и т. д. Одним из наиболее значительных преимуществ для киберпреступников во всем этом является то, что, хотя границы между интернет-средами взаимосвязаны, многие организации пожертвовали централизованной видимостью и унифицированным контролем в пользу производительности и цифровой трансформации. В результате киберзлоумышленники стремятся развивать свои атаки, ориентируясь на эти среды, и будут стремиться использовать возможности скорости и масштабирования.

[1] Wide Area Network — глобальная компьютерная сеть (Интернет).

В то время как конечные пользователи и их домашние ресурсы уже являются целями для киберпреступников, изощренные злоумышленники будут использовать их в качестве трамплина для других целей в будущем. Атаки на корпоративные сети, запущенные из домашней сети удаленного работника, особенно когда четко известны тенденции использования этой сети, можно тщательно координировать, чтобы они не вызывали подозрений. В конце концов, продвинутые вредоносные программы могут также обнаруживать еще более ценные данные и тенденции с помощью новых EAT (троянских программ пограничного доступа) и выполнять инвазивные действия, такие как перехват запросов из локальной сети для компрометации дополнительных систем или введения дополнительных команд атаки.

Компрометация и использование новых устройств с поддержкой 5G откроют возможности для более сложных угроз. Киберпреступники добиваются прогресса в разработке и развертывании атак на основе роя. В этих атаках используются захваченные устройства, разделенные на подгруппы, каждая из которых обладает специальными навыками. Они нацелены на сети или устройства как на интегрированную систему и обмениваются данными в режиме реального времени для уточнения своей атаки по мере ее проведения. Технологии роя требуют больших вычислительных мощностей для включения отдельных роевых ботов и эффективного обмена информацией в рое ботов. Это позволяет им быстро обнаруживать уязвимости, делиться ими и сопоставлять их, а затем менять методы атаки, чтобы лучше использовать то, что они обнаруживают.

«Умные» устройства или другие домашние системы, которые взаимодействуют с пользователями, будут не просто целями для атак, но и проводниками для более глубоких атак. Использование важной контекстной информации о пользователях, включая распорядок дня, привычки или финансовую информацию, может сделать атаки на основе социальной инженерии более успешными. Более «умные» атаки могут привести к гораздо большему эффекту, чем отключение систем безопасности, отключение камер или захват интеллектуальных устройств, они могут иметь целью выкуп и вымогательство дополнительных данных или скрытые атаки с учетными данными.

Программы-вымогатели продолжают развиваться, и по мере того, как IT-системы все больше объединяются с системами операционных технологий, особенно с критически важной инфраструктурой, программы-вымогатели будут угрожать еще больше. Вымогательство, клевета и вывод из строя уже стали причинами торговли программами-вымогателями. В будущем человеческие жизни окажутся под угрозой, когда полевые устройства и датчики на границе операционных технологий, которые включают в себя критически важные инфраструктуры, будут все чаще становиться целями киберпреступников на местах.

Также не за горами появление других типов атак, нацеленных на производительность вычислений и инновации в области связи, специально для получения выгоды киберпреступниками. Эти атаки позволят злоумышленникам охватить новую территорию и заставят защитников пытаться опередить киберпреступников.

Возможность подключения спутниковых телекоммуникаций может стать привлекательной целью для киберпреступников. По мере того как новые системы связи совершенствуются и начинают больше зависеть от спутниковых систем, киберпреступники могут использовать это в своих целях. В результате взлом спутниковых базовых станций и последующее распространение этого вредоносного ПО через спутниковые сети могут дать злоумышленникам возможность потенциально нацеливаться на миллионы подключенных пользователей в любом масштабе или проводить DDoS-атаки, которые могут приводить к сбою в работе жизненно важных коммуникаций.

С точки зрения кибербезопасности квантовые вычисления могут создать новый риск. Огромная вычислительная мощность квантовых компьютеров может сделать некоторые асимметричные алгоритмы шифрования разрешимыми. В связи с этим организациям необходимо будет подготовиться к переходу на квантово-устойчивые криптоалгоритмы, используя принцип криптогибкости, чтобы обеспечить защиту текущей и будущей информации. Средний киберпреступник не имеет доступа к квантовым компьютерам, однако в некоторых государствах возможная угроза может быть реализована, если сейчас не будут предприняты меры для противодействия ей посредством криптографической гибкости.

Глава 2. Киберустойчивость и противостояние кибермафии

2.1. Принципы киберустойчивости

К настоящему времени большинство предприятий осознают, что им необходимо инвестировать значительные суммы денежных средств и ресурсов в кибербезопасность. Коллективные глобальные расходы достигли 145 млрд долларов в год и, по прогнозам, к 2035 г. превысят 1 трлн долларов.

Поскольку количество и влияние кибератак продолжают расти, эксперты ВЭФ пришли к осознанию того, что в глобальном масштабе недостаточно делается для обеспечения кибербезопасности. Нынешняя ситуация сравнима с позиционной войной: прогресс идет медленно, а жертвы высоки.

Ни у одной компании нет ресурсов для решения всех киберпроблем, и не все меры одинаково актуальны. Только начав определять виды деятельности, которые важны для бизнеса, и понимая, как атаки могут помешать им, можно начать расставлять приоритеты в процессе снижения рисков.

К сожалению, многие компании пропускают этап выявления этих критически важных бизнес-операций, которые могут быть нарушены кибератакой, и вместо этого сосредоточиваются на отдельных технологиях для решения частных проблем в своих IT-системах.

Хотя уже существует множество руководств, направленных на оснащение специалистов по кибербезопасности инструментами и знаниями, необходимыми для управления киберрисками, руководители предприятий, особенно малых и средних, работающих в убыточных отраслях или регионах, часто с трудом понимают важность кибербезопасности и обязанности специалистов по кибербезопасности.

Киберустойчивость стала определяющим требованием нашего времени, включающим предвидение будущих угроз, противостоя-

ние кибератакам, восстановление после них и адаптацию к будущим цифровым потрясениям.

По мнению экспертов ВЭФ, руководители бизнеса должны быть готовы ответить на следующие вопросы.

Насколько хорошо мы готовы противостоять сбоям, связанным с кибератаками?

Насколько хорошо мы можем противостоять потере критически важных функций после кибератаки и как быстро мы можем их восстановить?

Три принципа помогут бизнес-лидерам внедрить киберустойчивость в свою организационную культуру и структуру.

1. Киберустойчивость должна регулироваться сверху.

У руководителей часто бытует мнение, что сфера кибербезопасности настолько сложна, что им придется делегировать полномочия. Устраняя пробел в киберграмотности, руководители предприятий смогут принимать более эффективные решения.

Компании также должны иметь в штате работника, который регулярно отчитывается непосредственно перед советом директоров о киберрисках и устойчивости к ним. Более того, совет директоров должен обсудить со своими специалистами по кибербезопасности критически важные бизнес-операции и любые угрозы, которые могут возникнуть. Важно точно знать, какие системы важны для данного бизнеса, чтобы помочь расставить приоритеты, вместо того чтобы перебирать уязвимости, которые необходимо ликвидировать.

Все руководители должны иметь информацию об известных атаках, о том, как они могут скомпрометировать бизнес, и о потенциальных экономических последствиях.

2. Киберустойчивость должна быть неотъемлемой частью операционной модели бизнеса.

Руководители предприятий должны начать рассматривать киберустойчивость как императив бизнеса, чтобы понять, какие активы и виды деятельности имеют решающее значение и обеспечивают конкурентное преимущество организации. Сбалансированный подход к киберустойчивости гарантирует, что инвестиции будут вкладываться не только в средства защиты и предотвращения кибератак, но также будут иметь приоритет в реагировании и восстановлении после серьезных нарушений кибербезопасности.

Профили киберрисков быстро развиваются из-за трансформационных инициатив и изменений в операционных моделях. Они различаются в зависимости от отрасли и сильно различаются в зависимости от продуктов и услуг, географии и нормативных требований, а также геополитического контекста.

Развивая киберграмотность своих сотрудников и адаптируя знания, необходимые сотрудникам, предприятия смогут лучше использовать возможности технологий, минимизируя риски, связанные с человеческим фактором.

Более того, компаниям необходимо наращивать внутренние возможности для работы с процессами управления изменениями и внедрять какой-либо тип гарантии киберрисков.

3. Киберустойчивость — фактор, способствующий достижению бизнес-результатов.

Нет гарантий, что практика кибербезопасности той или иной организации будет достаточной для отражения атаки, с которой она столкнется. Однако если руководители предприятий сосредоточатся на том, что важно для защиты, и поймут, какие атаки могут поставить под угрозу важные бизнес-операции, они с большей вероятностью смогут предвидеть и будут готовы снизить риск серьезной атаки и быстро восстановиться. Такая практика является непрерывной и динамичной и часто связана с изменениями в бизнесе — новыми партнерами в цепи поставок, новыми операционными моделями и т. д.

Более того, руководители предприятий должны искать ориентированные на ценность и результаты меры и показатели для оценки эффективности реализованных мер безопасности, окупаемости инвестиций в приобретенные технологии и услуги и их влияния на стратегические бизнес-результаты.

Чтобы полностью реализовать дивиденды цифровой трансформации, компании должны согласовать собственное видение со своей толерантностью к риску. Если риски безопасности, связанные с распространением технологической инфраструктуры и интернет-приложений, не будут должным образом сбалансированы с комплексными стратегиями кибербезопасности и планами устойчивости, предприятия не смогут добиться экономического роста и процветания, к которым они стремятся.

Главное направление в достижении киберустойчивости — это разработка новых инструментов борьбы с киберпреступностью в рамках действующих национальных структур и подходов.

Эксперты ВЭФ в новейших документах (май 2021 г.) призывают в целях кибербезопасности не откладывать на национальном уровне *переход на квантово-безопасные стандарты*, иначе все больше данных будет под угрозой.

«Мы используем криптографию для защиты инфраструктуры, обеспечения доверия к электронным транзакциям и защиты цифровых доказательств. Сегодня новые автомобили, самолеты и критически важная инфраструктура проектируются так, чтобы быть тесно связанными с цифровыми экосистемами, и ожидаемый срок службы составляет десятилетия. По мере того как наш мир становится все более взаимосвязанным и автоматизированным, мы становимся все более уязвимыми с точки зрения кибербезопасности. Будущая уязвимость в устаревшем компоненте, который не является квантово-безопасным, в случае компрометации может привести к массовым сбоям в работе» (ВЭФ, 7 мая 2021 г.).

2.2. Искусственный интеллект как ключевой элемент киберустойчивости

Эксперты ВЭФ подчеркивают, что эволюция искусственного интеллекта (ИИ) имеет решающее значение для защиты от новых кибератак в будущем. Технологии с улучшенным ИИ, которые могут видеть, предвидеть и противодействовать атакам, должны стать реальностью в будущем, потому что *кибератаки будущего будут происходить за микросекунды*. Основная роль людей будет заключаться в обеспечении того, чтобы системы безопасности получали достаточно информации, которая нужна не только для активного противодействия атакам, но и фактически для предвидения атак и их недопущения.

Тактика, приемы и процедуры субъектов угроз в виде сценариев могут быть переданы в системы ИИ для обнаружения шаблонов атак.

Эксперты Forbs считают, что применение ИИ особенно полезно при *атаках на два ключевых вектора электронной почты: саму электронную почту и приложения*. Изначально для электронной почты можно использовать ИИ и машинное обучение, чтобы

остановить атаки, которые маскируются под запросы и обновления, предлагающие открыть их или поделиться информацией об учетных данных. Совсем недавно специалисты по киберзащите стали использовать ИИ для изучения шаблонов электронной почты, чтобы определить, когда учетная запись электронной почты была взломана и начала использоваться для отправки атак другим жертвам. Многие злоумышленники используют ботов для поиска несанкционированного доступа к приложениям. В Интернете постоянно работают миллионы этих ботов, и ИИ используется для определения, какие из них являются вредоносными, а какие нет.

Искусственный интеллект окажется важным для решения проблем, связанных с *внедрением облачных технологий*. Поскольку ресурсы создаются и выключаются в течение нескольких часов или даже минут, группам IT-безопасности стало сложно управлять этими облачными разрешениями, т. е. устанавливать, кому, когда и в течение какого времени разрешен доступ к облачным рабочим нагрузкам. Традиционные инструменты часто неприменимы в этих новых средах. Тем не менее технология ИИ может помочь обнаружить риски, связанные с доступом, в средах «инфраструктура как услуга» (IaaS) и «платформа как услуга» (PaaS), обнаруживая как человеческие, так и машинные идентификаторы в облачных средах, а затем оценивая их права, роли и политики.

Искусственный интеллект чаще будет встроен в *системы аутентификации*. В контексте управления привилегированным доступом (PAM) мы знаем, что адаптивная многофакторная аутентификация (MFA) является одним из примеров, когда множество факторов аутентификации в сочетании с учетом динамического поведения пользователя может значительно снизить риск при принятии решений по аутентификации. В настоящее время это может привести к более частому использованию ИИ для определения оценок рисков в реальном времени и остановки угроз на этапе аутентификации, прежде чем они смогут нанести реальный ущерб.

Повышение прозрачности участников с открытым исходным кодом будет иметь решающее значение, а использование ИИ и машинного обучения станет катализатором для отсеивания тех, кто имеет злонамеренные цели.

У ИИ также есть возможность помочь *лучше продвигать конфиденциальность и улучшать технологии конфиденциальности*.

Благодаря ИИ *безопасность и IT-операции будут лучше интегрированы*. Алгоритмы безопасности моделируют исторические модели поведения и обнаруживают аномалии и отклонения от этих моделей практически в реальном времени. Используя ИИ, этот процесс можно автоматизировать для блокирования злоумышленников почти в реальном времени. Например, хакер пытается получить доступ или проникнуть через брандмауэр. Это обнаруживается либо по изменению объема данных, либо по изменению местоположения пользователя, который пытается получить к ним доступ. Чтобы классифицировать этот конкретный доступ как обычный, хакерский или небезопасный, можно использовать несколько функций. Как только злонамеренное действие будет обнаружено, эту информацию можно передать системе автоматизации/ИИ, чтобы заблокировать IP-адрес этого конкретного региона или этого конкретного диапазона.

Искусственный интеллект станет ключом к *укреплению киберустойчивости при удаленной работе.* Безопасность является приоритетом для руководства любой организации, которая вступила на путь цифровой трансформации, и важность безопасности только увеличилась из-за пандемии. С таким количеством конечных точек, разбросанных по всему миру, поскольку сотрудники могут работать удаленно, где бы они ни находились, уязвимости множатся. Основная тенденция, которую мы уже видим, — это применение ИИ к мерам безопасности, потому что люди в одиночку не могут отслеживать, контролировать и проверять каждую конечную точку для адекватной или эффективной защиты современного предприятия.

Управление идентификацией станет более рациональным, поскольку мы будем анализировать закономерности и аномалии для автоматизации запросов на доступ, выявления рискованных пользователей и устранения ручных и громоздких процессов повторной сертификации.

Глава 3. Основные направления международного сотрудничества в борьбе с кибермафией

3.1. Цели и задачи

Группа экспертов для проведения всестороннего исследования проблемы киберпреступности УНП ООН в апреле 2021 г. подготовила документ, который называется «Компиляция всех предварительных выводов и рекомендаций, предложенных государствами-членами в ходе совещаний Группы экспертов для проведения всестороннего исследования проблемы киберпреступности, проведенных в 2018, 2019 и 2020 годах».

Эти предварительные рекомендации и выводы сводятся к следующему.

Государствам следует обеспечить, чтобы их законодательные положения отвечали требованиям времени с учетом технического прогресса посредством принятия законодательства, содержащего технически нейтральные формулировки и предусматривающего *уголовную ответственность за деятельность, признаваемую незаконной, а не за использование технических средств.* Государствам-членам следует также рассмотреть вопрос о разработке согласованной терминологии для описания киберпреступной деятельности и содействия, насколько это возможно, точному толкованию соответствующего законодательства правоохранительными и судебными органами.

Государства должны уважать суверенные права других государств при разработке политики и законодательства, отвечающих их национальным особенностям и потребностям в области борьбы с киберпреступностью. Для содействия международному сотрудничеству в борьбе с киберпреступностью *принцип национального суверенитета не следует ошибочно трактовать как препятствие и рассматривать его скорее как основополагающий прин-*

цип и как исходное положение. Неустойчивый характер передачи и хранения электронных данных, например в «облаках», может потребовать участия в многосторонних обсуждениях вопроса об оказании государствами новаторской и расширенной взаимной помощи для обеспечения своевременного допуска к электронным данным и доказательствам.

Для предупреждения возникновения и (или) ликвидации «безопасных гаваней» для преступников государствам следует в максимально возможной степени сотрудничать друг с другом в таких областях, как расследование, сбор доказательств, уголовное преследование, вынесение судебного решения и в необходимых случаях изъятие незаконного контента из Интернета. Кроме того, государства должны обеспечивать максимально возможную гибкость своего международного сотрудничества для борьбы с киберпреступностью и другими видами преступности, связанными с использованием электронных данных, при ведении расследований или при обмене доказательствами независимо от того, как называются рассматриваемые виды деятельности в соответствующих государствах.

При разработке политики и законодательства государствам следует учитывать необходимость обеспечения баланса между защитой прав человека, с одной стороны, и соображениями, касающимися национальной безопасности, общественного порядка и законных прав третьих лиц, — с другой. Национальное законодательство, предусматривающее уголовную ответственность за деяния, связанные с киберпреступностью, и предоставление процессуальных полномочий на проведение расследований, возбуждение уголовного преследования и вынесение судебного решения по делам, связанным с киберпреступностью, должно обеспечивать соблюдение надлежащих процессуальных гарантий, принципов неприкосновенности частной жизни, гражданских свобод и прав человека. Национальная политика и национальное законодательство, а также существующие и (или) будущие международные документы должны быть основаны на многоаспектном подходе. С одной стороны, они должны включать адекватные меры борьбы с киберпреступностью, основанные на всестороннем понимании более широкого понятия кибербезопасности. С другой стороны, они должны не только охватывать противоправные деяния, но и должны быть направлены на предупреждение преступности, оказание помощи потерпевшим от преступной деятельности и содействие населению в целом. Для построения прочной основы международного сотрудничества в борьбе с киберпреступностью государствам-членам следует прилагать все усилия по формированию и развитию культуры, ориентированной на создание общего будущего для киберпространства.

Государствам следует осуществлять международное сотрудничество, не требуя при этом полного согласования национального законодательства при условии, что противоправное деяние является уголовно наказуемым, а законодательство — достаточно сопоставимым для упрощения и ускорения осуществления различных форм такого сотрудничества.

Государствам следует учитывать тот факт, что внутренняя нормативно-правовая база по-прежнему должна играть решающую роль в обеспечении эффективности и общей сбалансированности системы расследований и уголовного преследования, поскольку уголовное законодательство особенно восприимчиво к таким вопросам, как соблюдение основных свобод, и поскольку расследования в области компьютерных преступлений в существенной степени затрагивают частные сообщения и данные граждан.

Для обеспечения возможности уголовного преследования за совершение преступных деяний государствам следует в законодательном порядке ввести в действие *принцип экстратерриториальной юрисдикции* в отношении граждан или лиц, обычно проживающих на их территории, независимо от того, совершены ли эти деяния и являются ли они преступлениями в иностранной юрисдикции.

Государства, располагающие более широкими возможностями и развитой инфраструктурой в области борьбы с киберпреступностью, должны взять на себя ответственность, соразмерную этим возможностям или инфраструктуре, по оказанию правовой помощи другим государствам.

Для обеспечения должного учета соответствующих вопросов государствам-членам следует на возможно более раннем этапе консультироваться со всеми соответствующими заинтересованными сторонами, включая межправительственных субъектов, частный

сектор и гражданское общество, в тех случаях, когда принимается решение о принятии законодательства о киберпреступности.

Государствам следует развивать прочное и заслуживающее доверия государственно-частное сотрудничество в области борьбы с киберпреступностью, в том числе *сотрудничество между правоохранительными органами и поставщиками коммуникационных услуг.* Для укрепления и облегчения сотрудничества требуется также участие в диалоге с частными предприятиями в сочетании в случае необходимости с налаживанием государственно-частных партнерских отношений и заключением меморандумов о договоренности.

Государствам следует выделять достаточные ресурсы для наращивания национального потенциала. Надлежащее осуществление законодательства в борьбе с киберпреступностью требует *обучения сотрудников полиции и прокуроров, а также проведения информационно-пропагандистских кампаний.*

Деятельность государств-членов по наращиванию потенциала должна охватывать следующие области:

— обучение судей, прокуроров, следователей и сотрудников правоохранительных органов ведению расследований киберпреступлений, обращению с электронными доказательствами, обеспечению хранения и передачи доказательств и проведению судебной экспертизы;

— разработка, изменение и (или) осуществление законодательства о киберпреступности и электронных доказательствах;

— определение структуры подразделений, занимающихся расследованием киберпреступлений, и предоставление руководящих указаний в отношении соответствующих процедур;

— разработка, обновление и осуществление законодательства для *борьбы с использованием Интернета в террористических целях.*

Для укрепления международного сотрудничества как можно большему числу государств следует использовать существующие правовые документы и механизмы, включая Конвенцию ООН против транснациональной организованной преступности от 16 ноября 2000 г.

Следует учитывать тот факт, что *многие основные положения уголовного законодательства, применяемые к офлайновым преступлениям, могут также применяться к преступлениям, совершенным в режиме онлайн.*

Следует ввести уголовную ответственность за совершение основных киберпреступлений, которые воздействуют на конфиденциальность, целостность и доступность компьютерных сетей и компьютерных данных, с учетом широко признанных международных стандартов.

Следует рассмотреть вопрос о *криминализации*:

— новых или возникающих форм киберпреступной деятельности, таких как преступное использование криптовалют, преступления, совершаемые в даркнете и в Интернете вещей, фишинг и распространение зловредных программ и любого другого программного обеспечения, используемого для совершения преступных деяний;

— раскрытия личной информации и «порномести»;

— использования Интернета для совершения деяний, связанных с терроризмом;

— использования Интернета для подстрекательства к совершению преступлений на почве ревности и воинствующего экстремизма;

— оказания технической помощи или содействия в совершении киберпреступления;

— создания незаконных онлайновых платформ или публикации информации с целью совершения киберпреступлений;

— незаконного получения доступа к компьютерным системам или их взлома;

— незаконного перехвата или повреждения компьютерных данных и повреждения компьютерных систем;

— незаконного вмешательства в компьютерные данные и системы;

— неправомерного использования устройств;

— компьютерного подлога и мошенничества;

— нарушения авторских прав;

— сексуального принуждения и сексуальной эксплуатации детей и подстрекательства несовершеннолетних к совершению самоубийства;

— оказания незаконного воздействия на важнейшую информационную инфраструктуру.

Следует обеспечить возможность того, чтобы преступления, связанные с использованием компьютеров, рассматривались в специальных положениях, которые не просто предусматривают распространение применения положений о традиционных преступлениях на цифровую среду, а учитывают особенности цифровой среды и фактическую потребность в криминализации на основе тщательной оценки.

Главное внимание при международном согласовании положений, касающихся криминализации киберпреступлений, следует уделять основному своду преступлений против конфиденциальности, целостности и доступности информационных систем, притом что вопросы, связанные с необходимостью согласования порядка криминализации общих преступлений, совершаемых с использованием ИКТ, следует рассматривать главным образом на специальных форумах, посвященных конкретным областям преступности.

Следует взаимодействовать с провайдерами интернет-услуг и частным сектором для расширения сотрудничества с правоохранительными органами с учетом того факта, что большинство провайдеров интернет-услуг заинтересованы в том, чтобы их платформы не использовали преступники.

Важно принять и использовать на практике внутреннюю нормативно-правовую базу, касающуюся доказательств, которая позволяет считать *допустимыми электронные доказательства при проведении уголовных расследований и осуществлении уголовного преследования*, включая надлежащий обмен электронными доказательствами с иностранными правоохранительными органами-партнерами.

Следует изучить пути оказания помощи для своевременного и безопасного обмена информацией между следователями и прокурорами, занимающимися делами, связанными с киберпреступностью, в том числе посредством укрепления сетей национальных учреждений, которые могут работать круглосуточно.

Учитывая, что для ликвидации рынков киберпреступности требуются среднесрочные и долгосрочные стратегии правоохранительной деятельности, включая сотрудничество с международными партнерами, эти стратегии должны быть упреждающими и *преимущественно ориентированными на борьбу с организованными киберпреступными группами*, члены которых могут находиться во многих странах.

Развитие внутреннего процессуального права должно идти в ногу с развитием технологий и обеспечивать правоохранительным органам надлежащую оснащенность для борьбы с интернет-преступностью. *Соответствующие законы следует разрабатывать* с учетом применимых технических концепций и практических потребностей следователей, занимающихся расследованием киберпреступлений, при условии обеспечения соблюдения надлежащей правовой процедуры, неприкосновенности частной жизни, гражданских свобод и прав человека, а также принципов соразмерности и субсидиарности и гарантий, обеспечивающих судебный надзор.

Необходимо принять внутреннее законодательство, которое признает законными:

— просьбы об оперативном обеспечении сохранности компьютерных данных, направляемые лицу, осуществляющему контроль над этими данными, т. е. поставщикам интернет-услуг и услуг связи, с целью сохранения и обеспечения целостности этих данных в течение определенного периода времени;

— поиск и выемку хранимых данных с цифровых устройств, которые часто являются наиболее актуальными доказательствами совершения электронного преступления;

— распоряжения о предоставлении информации в электронной форме, которая может иметь меньшую степень защиты неприкосновенности частной жизни, такой как технические параметры трафика и абонентские данные;

— сбор технических параметров трафика и контента в режиме реального времени в соответствующих случаях.

Важно руководствоваться гибкими подходами к применимым юрисдикционным основам в области борьбы с киберпреступностью, в том числе в большей степени *учитывать место предоставления услуг в сфере ИКТ, а не место нахождения данных.*

Следует принять меры для поощрения участия поставщиков интернет-услуг в предупреждении киберпреступности и оказании поддержки правоприменительной деятельности и следственных мероприятий, в том числе путем установления во внутреннем законодательстве соответствующих положений относительно обязательств этих поставщиков услуг, и четко определить сферу и границы таких обязательств с целью защиты законных прав и интересов поставщиков услуг.

Необходимо усилить следственную и правоприменительную деятельность в отношении актов пособничества, подстрекательства и подготовки к совершению киберпреступлений, с тем чтобы эффективно противодействовать киберпреступности.

Следует разработать и применять юридические полномочия, юрисдикционные и другие процессуальные нормы в целях эффективного расследования киберпреступлений. Это могут быть:

— корректировка правил доказывания для обеспечения того, чтобы электронные доказательства можно было собирать, сохранять, аутентифицировать и использовать в уголовном производстве;

— принятие положений об отслеживании электронных сообщений на национальном и международном уровнях;

— принятие положений, регламентирующих произведение внутренних и международных обысков;

— принятие положений о перехвате электронных сообщений, передаваемых с использованием компьютерных сетей и аналогичных средств массовой информации;

— принятие норм материального и процессуального права, не связанных с конкретными технологиями, чтобы страны могли бороться с новыми и появляющимися формами киберпреступности.

Допустимость электронных доказательств не должна зависеть от того, были ли они собраны за пределами юрисдикции страны, при условии, что достоверность доказательств не снижена и доказательства собраны законно, например на основании договора о взаимной правовой помощи или многостороннего соглашения или в сотрудничестве со страной, обладающей юрисдикцией.

Для развития международного сотрудничества с использованием доказательств в электронной форме следует использовать такие существующие механизмы, как круглосуточные каналы связи и сотрудничество по линии Международной организации уголовной полиции (Интерпола), а также договоры о взаимной правовой помощи.

Следует принять меры по расширению сотрудничества в сборе доказательств в электронной форме, включая следующие:

— обмен информацией об угрозах киберпреступности;

— обмен информацией об организованных киберпреступных группах, в том числе об используемых ими приемах и методах;

— содействие укреплению сотрудничества и координации между правоохранительными органами, прокуратурой и судебными органами;

— обмен информацией о национальных стратегиях и инициативах по борьбе с киберпреступностью, в том числе о внутреннем законодательстве и порядке привлечения киберпреступников к ответственности;

— обмен передовой практикой и опытом в отношении трансграничных расследований киберпреступлений;

— развитие сети координаторов, объединяющей правоохранительные органы, судебные органы и прокуратуру;

— согласование и рационализация процедур, касающихся взаимной правовой помощи, и разработка общей схемы для ускорения процедуры оперативного сбора и передачи трансграничных доказательств в электронной форме;

— проведение практикумов и семинаров с целью повышения способности правоохранительных и судебных органов составлять запросы в контексте договоров о взаимной правовой помощи относительно сбора доказательств по вопросам, касающимся киберпреступлений;

— установление стандартов и единообразия в процедурных аспектах сбора и передачи доказательств в цифровой форме;

— разработка общего подхода к механизмам обмена информацией с поставщиками услуг в связи с расследованием киберпреступлений и сбором доказательств;

— взаимодействие с поставщиками услуг в рамках публично-частных партнерств с целью установления форм сотрудничества в правоохранительной сфере, расследовании киберпреступлений и сборе доказательств;

— разработка руководящих принципов для поставщиков услуг с целью содействия правоохранительным органам в расследовании киберпреступлений, в том числе в отношении формата и сроков обеспечения сохранности доказательств и информации в цифровой форме;

— укрепление технического и правового потенциала правоохранительных и судебных органов и прокуратуры с помощью программ по наращиванию потенциала и повышению квалификации;

— укрепление потенциала в области компьютерной криминалистики (форензики), в том числе путем создания лабораторий компьютерной криминалистики.

Государства могут рассмотреть вопрос о том, что в их внутреннем законодательстве *в качестве электронных доказательств будут признаны следующие данные*:

— технические параметры трафика, например файлы регистрации;

— содержание информации, например электронных писем;

— сведения об абонентах, например информация о регистрации пользователей;

— другие данные, которые хранятся, обрабатываются и передаются в цифровом формате и которые создаются во время совершения преступления и поэтому могут использоваться для подтверждения фактов этого преступления.

Государствам рекомендуется:

— повышать способность осуществлять сбор электронных доказательств, создавать группы специалистов, обладающих как юридическими, так и техническими знаниями, и расширять сотрудничество в области обмена опытом и профессиональной подготовки. УНП ООН рекомендуется принимать участие в этой деятельности;

— предусмотреть в своем внутреннем законодательстве соответствующие методы сбора электронных доказательств, такие как выемка и обеспечение сохранности оригинального носителя, сбор на месте, дистанционный сбор и верификация;

— производить фиксацию электронных доказательств для предотвращения их добавления, уничтожения или изменения с помощью таких мер, как вычисление контрольной суммы электронного доказательства, блокировка учетных записей веб-приложений и установление защиты от записи;

— установить технические нормы и стандарты для сбора электронных доказательств;

— обеспечить, чтобы сбор электронных доказательств осуществлялся с соблюдением надлежащей процедуры;

— установить правила оценки подлинности, целостности, законности и актуальности электронных доказательств и учитывать специфику электронных доказательств при применении правил,

касающихся первичных доказательств, показаний с чужих слов и исключения доказательств, полученных незаконным путем;

— при сборе электронных доказательств за рубежом уважать суверенитет государств, в которых находятся данные, соблюдать надлежащую процедуру и уважать законные права соответствующих лиц и организаций. В связи с этим следует также воздерживаться от одностороннего применения интрузивных или деструктивных технических методов при производстве следственных действий;

— разработать адекватные и по возможности единообразные правила и сроки удерживания/хранения данных, чтобы обеспечить возможность получения или обеспечения сохранности электронных доказательств, необходимых для обоснования последующих просьб о взаимной правовой помощи;

— организовать ведение электронных баз данных для облегчения доступа к статистическим данным по входящим и исходящим запросам о взаимной правовой помощи, связанной с электронными доказательствами, с целью обеспечить возможность оценки эффективности;

— действовать через центральные органы при передаче просьб о взаимной правовой помощи и взаимодействии с компетентными органами по вопросам их выполнения с целью соблюдения требований действующих договоров и сокращения задержек в процессе работы;

— не допускать использования ИКТ в качестве оружия, осудить совершение кибератак при поддержке государств и привлекать к ответственности стоящих за ними лиц;

— создать механизм быстрого реагирования и канал связи для оказания судебной помощи и сотрудничества между правоохранительными органами в борьбе с киберпреступностью и рассмотреть возможность обмена правовыми документами и электронными доказательствами в онлайн-режиме при условии их удостоверения электронными подписями и с помощью других технических средств;

— препятствовать выводу незаконных доходов от киберпреступлений за рубеж и укреплять международное сотрудничество в области возвращения активов, связанных с киберпреступностью.

Предупреждение киберпреступности является обязанностью не одного государства, требует участия всех заинтересованных сторон, включая правоохранительные органы, частный сектор, особенно поставщиков интернет-услуг, неправительственные организации, учебные заведения, научные круги и рядовых граждан.

Рекомендовано:

— обеспечить, чтобы у граждан был доступ к таким инструментам предупреждения киберпреступности, как онлайн-платформы, аудиоклипы и наглядные информационные материалы, изложенные простым и понятным языком, а также платформы для сообщения о нарушениях;

— разработать долгосрочные государственные стратегии предупреждения киберпреступности, предусматривающие проведение информационных кампаний на тему безопасного пользования Интернетом;

— тему кибербезопасности включить в программу образовательных организаций начального, среднего и высшего образования для повышения осведомленности учащихся и преподавателей. В идеале такую работу следует проводить в рамках национальной стратегии кибербезопасности;

— предусматривать в национальных стратегиях противодействия киберпреступности такие направления работы, как предупреждение киберпреступности, развитие государственно-частного партнерства, укрепление потенциала системы уголовного правосудия и повышение осведомленности путем публикации судебных решений;

— принять конкретные и целенаправленные меры для обеспечения безопасности детей в Интернете. В рамках такой работы необходимо обеспечить, чтобы национальная нормативно-правовая база, практические договоренности и механизмы международного сотрудничества обеспечивали возможность сообщать о фактах сексуальных надругательств над детьми и эксплуатации детей в Интернете, выявлять и расследовать такие факты, осуществлять уголовное преследование в связи с ними и принимать сдерживающие меры;

— уделять особое внимание проведению профилактической работы с молодежью, в том числе с лицами, впервые совершившими правонарушения, ради профилактики рецидивизма;

— уделять особое внимание профилактике и пресечению гендерного насилия, в частности насилия в отношении женщин и девочек, и преступлений на почве ненависти;

— профилактическую работу проводить с учетом интересов социально уязвимых категорий населения;

— четко определить обязанности поставщиков интернет-услуг по выявлению, предотвращению и пресечению киберпреступлений;

— вести сбор данных по широкому спектру вопросов для обеспечения лучшего понимания тенденций с целью выработки обоснованной политики и оперативных мер борьбы с киберпреступностью;

— разрабатывать и развивать программы поддержки жертв киберпреступлений;

— проводить опросы для оценки воздействия киберпреступности на бизнес, в том числе для сбора информации о принимаемых мерах, подготовке сотрудников, видах инцидентов в сфере кибербезопасности, с которыми сталкиваются коммерческие предприятия, и расходах на предотвращение подобных инцидентов и устранение их последствий;

— оказывать поддержку бизнесу и профессиональным сообществам в повышении осведомленности о рисках киберпреступности, реализации стратегий смягчения последствий кибератак и совершенствовании методов работы в киберпространстве;

— внимательно изучать способы совершения киберпреступлений путем анализа оперативных данных и проведения криминологических исследований с целью более эффективного использования имеющихся ресурсов и выявления уязвимостей;

— создать координационную платформу для мгновенного обмена данными о выявленных инцидентах и новых тенденциях в сфере киберпреступности;

— создать криминалистические наблюдательные центры для отслеживания угроз и тенденций киберпреступности;

— на регулярной основе выпускать бюллетени с информацией о предотвращенных инцидентах и доводить их до сведения пользователей, организаций и других заинтересованных сторон с целью содействия предотвращению инцидентов в сфере кибербезопасности, потенциально способствующих преступной деятельности;

— использовать искусственный интеллект для создания систем, которые будут автоматически менять конфигурацию при обнаружении кибератаки;

— создать глобальную базу данных о нарушениях, связанных с криптовалютой и использованием больших массивов данных в преступных целях, а также согласованно провести глобальный стратегический обзор угроз, создаваемых преступной деятельностью в даркнете;

— проводить более активную информационную работу по проблеме киберзапугивания и угроз применения насилия и жестокого обращения в Интернете и оказывать помощь нормотворческой деятельности, направленной на борьбу с этими явлениями;

— для обобщения национального и регионального опыта создать многосторонний банк данных, который будет способствовать распространению передовой практики, выработанной в разных контекстах.

3.2. Электронные доказательства: международные механизмы их получения

Как могут быть получены электронные доказательства, если они хранятся у поставщика связи, находящегося в другой стране? Как сохранить электронные доказательства до их удаления или изменения в формате? Как можно быстро получить данные от провайдера для предотвращения чрезвычайной ситуации?

В целях наращивания потенциала следователей и прокуроров во всем мире УНП ООН, Исполнительный директорат Контртеррористического комитета ООН (ИДКТК) и Международная ассоциация прокуроров (МАП) совместно разработали и ввели в действие в 2019 г. *Практическое руководство для запроса электронных доказательств через границы*, в котором содержатся ответы на обозначенные вопросы.

Практическое руководство, разработанное в сотрудничестве с государствами, другими международными и региональными организациями и поставщиками коммуникационных услуг, такими как Facebook (Meta), Google, Microsoft и Uber, содержит информацию, которая поможет определить шаги на национальном уровне для сбора, сохранения и обмена электронными доказательствами с

общей целью обеспечить эффективность практики взаимной правовой помощи.

Интернет, социальные сети и системы мгновенного обмена сообщениями (мессенджеры) постоянно развиваются. Преступники хотят обеспечить сохранение своей анонимности и используют любую технологию, которая помогает этого достичь. В Руководстве описываются некоторые из таких проблем и варианты реагирования на них. Обязанность практикующих специалистов — всегда оставаться в курсе соответствующих изменений, реформ национального законодательства, а также процедур поставщиков услуг, чтобы иметь возможность получить необходимые им электронные доказательства.

В своих резолюциях Совет Безопасности ООН призвал государства — члены ООН собирать и сохранять доказательства, чтобы обеспечить возможность проведения расследований и судебного преследования для привлечения к ответу лиц, ответственных за террористические атаки.

Электронные доказательства, хранящиеся у поставщиков услуг, могут быть использованы для подтверждения того, что преступление было совершено, для раскрытия сведений об обличающих связях и определения местонахождения правонарушителей. Получение таких электронных доказательств поможет обеспечить судебное преследование конкретного виновного лица, а также привлечение к ответственности лиц, совершающих серьезные преступления. Чрезвычайно важно учитывать на раннем этапе возможность запроса доказательств у иностранного поставщика услуг, поскольку такие расследования могут потребовать много времени, оказаться сложными и дорогостоящими. Часто это означает обращение за взаимной правовой помощью (ВПП), и означенный механизм становится все более перегруженным, что приводит к значительным задержкам. Это никак не сочетается со стремительным характером терроризма или организованной преступности, для которых в Интернете нет границ.

Практикующим специалистам в запрашивающем государстве (а именно сотрудникам правоохранительных органов, прокуратуры и судебных органов) необходимо понимать, как сохранить электронные доказательства, получить данные, чтобы предотвратить чрезвычайную ситуацию, как и когда использовать альтернативы

ВПП, а также как составить соответствующий запрос на оказание ВПП (ЗВПП) в отношении электронных доказательств. Аспект развития компетенций в этих сферах сохраняет свою важность, поскольку отдельные правительства и региональные органы начинают разрабатывать новые, дополнительные структуры для получения электронных записей.

Цель Руководства состоит в оказании содействия практикующим специалистам, а именно следователям, сотрудникам прокуратуры, сотрудникам судебных органов, а также компетентных национальных органов власти, ответственных за организацию взаимной правовой помощи (центральных органов) государств — членов ООН в области обеспечения сохранности и получения электронных доказательств от поставщиков услуг, располагающихся в иностранных юрисдикциях.

Руководство было составлено, чтобы обеспечить соответствие международному праву, включая международное право в области прав человека, и принимает во внимание соблюдение права на неприкосновенность частной жизни и свободу выражения мнений. Это означает, что *запрос электронных доказательств должен:*

— быть законным в соответствии с законами и процедурами запрашивающего и запрашиваемого государств, а также в соответствии с их международными обязательствами по соблюдению прав человека;

— быть необходимым для содействия в судебном преследовании лица, совершившего преступление, или для доказательства невиновности подозреваемого, а также в целях сопоставимого масштаба ущерба от киберпреступления;

— учитывать воздействие на третьих лиц и не допускать вторжения в частные взаимоотношения лиц, не являющихся объектами расследования;

— находиться под действием систем независимого надзора со стороны как судебных механизмов, так и других органов, уполномоченных обеспечивать правомерное поведение правоохранительных органов и спецслужб.

Электронные доказательства могут оказаться важными для определения того, где и с кем находится подозреваемый, с кем он поддерживает связь. Результаты исследования в Европейском Союзе подтвердили, что:

— в рамках более половины расследований направляется запрос на получение трансграничного доступа к электронным доказательствам;

— электронные доказательства в любой форме имеют большое значение приблизительно для 85% от общего числа (уголовных) расследований;

— почти в двух третях (65%) расследований, в рамках которых важно получить электронные доказательства, необходимо направить запрос поставщику услуг, располагающемуся в другой юрисдикции;

— облачные вычисления создают проблемы, связанные с определением юрисдикции, что подразумевает особое внимание к тому, куда направлять ЗВПП для исполнения.

Электронные доказательства быстро перемещаются через границы, а получение соответствующих сведений посредством ВПП нередко происходит медленно и представляет собой трудоемкую задачу, особенно если практикующий специалист не имеет опыта в осуществлении процедуры ВПП. Учитывая, что число трансграничных преступлений растет, а электронные доказательства нередко располагаются за границей, Руководство снабжает сотрудников правоохранительных органов и прокуратуры инструментами, которые помогут запрашивать эти важные доказательства. Такими инструментами являются:

— краткий обзор процедур крупных поставщиков услуг в отношении обеспечения сохранности электронных доказательств, чтобы создать возможность запросить их незамедлительно;

— прямые запросы поставщикам услуг или использование механизмов сотрудничества между полицейскими службами для раскрытия электронных доказательств (без необходимости направлять ЗВПП), чтобы сократить задержки;

— сведения о том, как долго абонент использовал эту конкретную услугу, а также IP-адрес, с которого впервые был совершен вход в систему;

— метаданные, связанные с оказанием услуг, включая данные, касающиеся подключения, трафика или местоположения коммуникации (например, IP-адрес или MAC-адрес);

— журналы регистрации доступа, в которых указываются время и дата осуществления доступа к услуге конкретным физиче-

ским лицом, а также IP-адрес, с которого осуществлялся доступ к услуге;

— журналы операций, в которых фиксируются продукты или услуги, полученные конкретным физическим лицом от поставщика или третьего лица (например, приобретение места в облачном хранилище).

Обеспечение сохранности подразумевает создание «снепшота» (снимка) учетной записи пользователя, который необходимо сохранить в момент получения и обработки запроса поставщику услуг. Чтобы обеспечить оперативность этого процесса во избежание удаления информации или изменения формата пользователем, многие поставщики услуг позволяют правоохранительным органам связываться с ними напрямую по вопросам обеспечения сохранности электронных доказательств.

Чрезвычайно важно установить, куда следует направлять запрос об обеспечении сохранности. Поставщик услуг может хранить данные в разных странах мира, но это не значит, что запрос об обеспечении сохранности следует направлять туда, где поставщик услуг хранит данные. Запрос об обеспечении сохранности следует направлять туда, где поставщик услуг осуществляет распоряжение и управление данными.

С учетом объема услуг, оказываемых пользователям, некоторые поставщики услуг хранят лишь ограниченный объем данных в течение короткого периода времени.

В качестве примеров можно назвать Snapchat и WhatsApp. Необходимо убедиться в том, что электронные доказательства все еще хранятся у поставщика услуг, направив обращение к его руководству о порядке взаимодействия с правоохранительными органами или в рамках сотрудничества между полицейскими службами. Поставщик услуг лишь сохранит то, что хранится в учетной записи на момент обеспечения сохранности, и не будет проводить никаких проверок относительно того, содержит ли такая учетная запись какие-либо данные. Такая информация о содержании удаляется сразу же после просмотра всеми получателями или через 30 дней после отправки, если сообщение не будет открыто. Так, WhatsApp не хранит сообщения после их доставки и открытия, а также информацию о трафике в отношении таких доставленных сообщений.

Недоставленные сообщения стираются с серверов WhatsApp через 30 дней.

Еще одной проблемой, которую следует принимать во внимание, является тяжесть уголовного преступления. Некоторые государства не выполняют ЗВПП в отношении незначительных дел в силу ограничений, установленных законодательством или практикой. Если расследуемое преступление не предусматривает выполнения ЗВПП, поставщики услуг имеют право не сохранять электронные доказательства.

Например, в США, как правило, не выполняются ЗВПП в отношении преступлений, срок заключения по которым составляет 12 месяцев и менее или которыми был причинен ущерб на сумму менее 5000 долларов США.

Обеспечение сохранности следует осуществлять незамедлительно, или электронные доказательства могут быть удалены либо их формат может быть изменен пользователем и их нельзя будет использовать в суде.

Если пользователь удалил сообщение, поставщик услуг может хранить его не дольше 48 часов. Это означает, что, как только поставщик услуг удалит или очистит электронные доказательства со своего сервера, восстановить их будет невозможно. Во избежание необратимой потери электронных доказательств в результате их удаления необходимо придавать процедуре обеспечения сохранности первостепенное значение.

Подготовка и направление запроса об обеспечении сохранности могут быть выполнены:

— сотрудником иностранного правоохранительного органа, прокуратуры или судебного органа посредством прямого контакта с поставщиком услуг;

— в рамках сотрудничества между полицейскими службами или по иным каналам (когда возможность для прямого контакта с поставщиком услуг отсутствует) посредством использования, например, сети Интерпола i24/7;

— посредством направления ЗВПП, когда законы или политика запрашиваемого государства не допускают прямого контакта с поставщиком услуг со стороны запрашивающего государства, а обращение посредством системы сотрудничества между полицейскими службами невозможно.

Направление ЗВПП об обеспечении сохранности данных — значительно более медленный процесс, чем прямой контакт или обращение посредством системы сотрудничества между полицейскими службами. Если необходимо направить ЗВПП, в рамках ЗВПП следует уделить особое внимание просьбе о выдаче надлежащего распоряжения суда о незамедлительном предоставлении данных, а не просто обратиться с запросом об обеспечении сохранности.

Если запрос об обеспечении сохранности направляется напрямую поставщику услуг, существует возможность того, что владелец интересующей учетной записи может узнать об этом — автоматически вследствие технических возможностей сервера поставщика услуг или потому, что уведомление владельца учетной записи вручную в таких случаях является политикой поставщика услуг. Однако в большинстве случаев исполнение запроса об обеспечении сохранности не будет очевидным для клиентов крупных и хорошо известных поставщиков услуг.

Большинство поставщиков услуг требуют от лиц, направляющих запрос, использовать официальный адрес электронной почты государственного ведомства или правоохранительного органа.

Онлайн-порталы (при наличии таковых) являются самым быстрым и эффективным способом связи с поставщиком услуг и должны использоваться в качестве предпочтительного метода при любой возможности.

Как только данные учетной записи будут сохранены, такому сохранению, как правило, присваивается ссылочный номер. Его следует включать во все письма поставщику услуг, например в отношении продления срока обеспечения сохранности. Кроме того, это ссылочный номер для исходного сохранения, а сведения о любом продлении срока обеспечения сохранности следует включать в ЗВПП, чтобы убедиться в обеспечении сохранности запрашиваемых электронных доказательств. Во вручаемое поставщику услуг распоряжение суда в запрашиваемом государстве будет включен ссылочный номер сохранения, использованный в ЗВПП, чтобы поставщик услуг знал, где можно быстро найти соответствующие электронные доказательства.

Если законодательством государства не предусмотрены положения в отношении обеспечения сохранности, в целях получения

электронных доказательств запрашивающее государство может в срочном порядке обратиться за выдачей распоряжения о предоставлении информации или ордера на обыск и выемку. Или же, при наличии связи между расследованиями в запрашивающем и запрашиваемом государствах, может быть получено судебное распоряжение о предоставлении информации и (или) выемке в рамках внутреннего расследования в запрашиваемом государстве, а результат расследования может быть предоставлен запрашивающему государству.

Направляя запрос об обеспечении сохранности поставщику услуг, надо помнить, что не все они заслуживают доверия. Важно отметить, что во многих государствах отрасль поставки услуг регулируется в малой степени. Существуют примеры, когда поставщиком услуг фактически управляет преступное предприятие, и в этом случае направление запроса об обеспечении сохранности может привести к предупреждению лица, в отношении которого проводится расследование. Таким образом, прежде чем направлять прямой запрос неизвестному поставщику услуг, следует рассмотреть возможность использования более подходящего способа для обеспечения сохранности.

Независимо от выбранного метода, как только запрос об обеспечении сохранности будет направлен, сотрудники правоохранительных органов, прокуратуры или судебных органов должны начать применять один из методов получения электронных доказательств (прямой запрос или направление ЗВПП).

Интерпол рекомендует государствам (если это допускается их правовой системой) назначить национальную группу экспертов или единый контактный центр, которые смогут сотрудничать с поставщиком услуг в другом государстве. Это позволит не допустить обращения с запросом об обеспечении сохранности со стороны более чем одного национального ведомства в рамках нескольких расследований, а также обеспечит сохранность электронных доказательств. Большинство поставщиков услуг также рекомендуют использовать эту практику.

Запрос на оказание ВПП не требуется автоматически для получения электронных доказательств от поставщиков услуг во всех иностранных государствах. Их можно попробовать *получить более быстрым способом*, таким как:

— поиск в открытых источниках;

— прямые запросы поставщику услуг;

— прямой контакт с пользователем учетной записи в отношении предоставления электронных доказательств, которые он скачивает из своей учетной записи;

— согласие пользователя учетной записи или его ближайшего родственника, чтобы поставщик услуг предоставил электронные доказательства из учетной записи;

— сотрудничество между полицейскими службами, обеспечиваемое полицией запрашиваемого государства на основании судебного решения или в рамках добровольного раскрытия информации.

Тот факт, что электронные доказательства не запрашиваются в рамках оказания ВПП, не означает, что данные предоставляются «только для сведения» или не предназначены «для использования в суде». Речь идет о методе получения доказательства, т. е. не посредством ЗВПП. Необходимо подчеркнуть: прежде чем получать электронные доказательства из другого государства без использования ЗВПП, представители запрашивающего государства должны убедиться в том, что:

— они не совершают уголовно наказуемого деяния в государстве, запрашивая данные напрямую, или что поставщик услуг не нарушает закон запрашиваемого государства, раскрывая данные;

— получение электронных доказательств способами, не предусматривающими оказание ВПП, подходит для той цели, с которой оно осуществляется запрашивающим государством.

Запрос на оказание ВПП необходим, если получение электронных доказательств в принудительном порядке или по распоряжению суда является законодательным требованием, обеспечивающим представление приемлемых для суда электронных доказательств в запрашивающем государстве.

Прежде чем запрашивать электронные доказательства в другом государстве, нужно убедиться в том, что возможности на национальном уровне уже исчерпаны. Это включает осуществление поиска в открытых источниках, чтобы:

— определить местоположение пользователя с помощью общедоступных онлайн-инструментов, таких как IP-адрес;

— установить владельцев доменных имен;

— доказать совершение преступления через учетные записи в общедоступных социальных сетях. Такие доказательства могут варьироваться от изображений или видеороликов, размещенных физическими лицами, до публикаций, уличающих в преступном поведении.

Поставщики услуг также могут раскрыть электронные доказательства сотруднику правоохранительного органа, прокуратуры или судебного органа запрашивающего государства в следующих ситуациях, не являющихся чрезвычайными:

— с согласия пользователя;

— в случае смерти пользователя и если его или ее ближайший родственник даст согласие на раскрытие информации и будет получено распоряжение суда запрашивающего государства о предоставлении информации;

— по прямому запросу в адрес поставщика услуг в отношении основной информации об абоненте (ОИА) или информации о трафике, направленному сотрудником иностранного правоохранительного органа, прокуратуры или судебного органа.

Важно, чтобы сотрудник иностранного правоохранительного органа, прокуратуры или судебного органа указал в прямом запросе поставщику услуг следующую информацию:

— запрашиваемые электронные доказательства и идентификаторы пользователя/учетной записи у конкретного поставщика услуг;

— определенный временной интервал для информации о трафике;

— отношение ОИА и (или) информации о трафике к соответствующему правонарушению;

— кто санкционировал направление прямого запроса. Это может быть старший сотрудник правоохранительного органа, прокурор или следственный судья;

— указание в отношении того, кому следует передать ОИА и (или) информацию о трафике;

— указание в отношении того, требуется ли заявление или аффидевит, подтверждающие подлинность запрашиваемых электронных доказательств (в случае отсутствия самоаутентификации).

Если это требуется поставщику услуг для добровольного раскрытия информации (например, в случае Microsoft, Snapchat и

Twitter), должно прилагаться подписанное распоряжение суда (переведенное на английский язык) об истребовании ОИА и (или) информации о трафике, полученное в запрашивающем государстве.

Если ОИА или информация о трафике была получена у поставщика услуг по прямому запросу на добровольное раскрытие информации, сотрудник прокуратуры, составляющий ЗВПП, должен указать помимо прочих доказательственных оснований, что такие электронные доказательства соответствуют правовому стандарту в отношении содержания, а также подтвердить, что поставщик услуг ранее сотрудничал со следствием.

Следует всегда учитывать, могут ли данные, полученные с согласия пользователя или по прямому запросу, быть представлены в качестве доказательств. По запросу поставщики услуг могут предоставить подтверждающее заявление, чтобы установить происхождение электронных доказательств. Некоторые поставщики услуг обеспечивают самоаутентификацию электронных доказательств, а другие не могут представить такую информацию. Если результат добровольного раскрытия информации нельзя использовать в суде, может потребоваться ЗВПП, чтобы обеспечить представление электронных доказательств в формате, требуемом для судебных разбирательств в запрашивающем государстве.

Политика поставщика услуг в области уведомления пользователей не очевидна в части прямых запросов, поэтому поставщика услуг необходимо проинструктировать о том, чтобы он не уведомлял пользователя, если это повлияет на расследование. Следует указать конкретные причины того, почему уведомление пользователя окажет такое влияние: например, уведомление пользователя предупредит его о скрытом расследовании и приведет к уничтожению электронных доказательств.

Если расследование является конфиденциальным или скрытым, возможно, наилучшим выбором будет направить ЗВПП в отношении выдачи распоряжения суда, чтобы обеспечить конфиденциальность. Этот аспект следует оценивать в индивидуальном порядке, чтобы определить подходящий порядок действий. Однако в тех случаях, когда пользователя можно уведомить (т. е. он уже арестован/допрошен в отношении доказательств, а сохранность данных учетной записи уже обеспечена), поставщика услуг следует проинформировать о том, что уведомление пользователя проблемой не является.

Для организации сотрудничества между полицейскими службами и обмена сведениями и оперативными данными доступно несколько каналов, наиболее значимыми из них представляются: национальные компетентные органы (в некоторых государствах называются «уполномоченные единые контактные центры»), канал региональных/межрегиональных органов (например, национальные центральные бюро Интерпола или Европола), а также канал офицеров связи.

В разных государствах используются различные стандартные операционные процедуры, которые не регулируются единым международным документом. Некоторые государства не требуют наличия конкретных юридических документов для сотрудничества с другими государствами в целях обеспечения работы органов правопорядка, и неофициальное сотрудничество возможно. Однако было замечено, что официальное соглашение любого типа (например, меморандум о взаимопонимании) нередко рассматривается как необходимое условие для сотрудничества между полицейскими службами. На тех же принципах может осуществляться сотрудничество между прокуратурами и судебными органами в разных государствах.

Обмен информацией между офицерами связи — быстрый канал, и именно его предпочитают использовать на этапе предварительного следствия в случаях, когда между двумя государствами заключено двустороннее соглашение, которое предусматривает такие формы сотрудничества и обмена информацией. Сотрудничество между полицейскими службами может оказаться быстрым способом получить ОИА и информацию о трафике. Государство, получающее любые данные в рамках сотрудничества между полицейскими службами, должно определить, могут ли такие данные использоваться в качестве доказательств и соответствуют ли они законодательству запрашиваемого государства, если требуют конфиденциального обращения.

Если такие данные нельзя использовать в качестве доказательств, их также можно использовать:

— для подтверждения того, что электронные доказательства существуют и должны быть сохранены;

— для определения или исключения соответствующих линий расследования;

— в ЗВПП в отношении электронных доказательств в качестве подтверждающих оснований для выдачи распоряжения суда о раскрытии данных поставщиком услуг.

Язык ЗВПП — это язык официального юридического документа, который должен быть понятным и исполнимым для запрашиваемого государства. Запрашиваемому государству следует предоставить всю информацию, необходимую ему для принятия решения об оказании помощи и порядке ее оказания. Нужно использовать официальные и вежливые формулировки. При использовании аббревиатур их всегда необходимо расшифровывать при первом упоминании. Хотя просторечных и жаргонных выражений в целом следует избегать, важно использовать формулировки, присущие соответствующему типу запрашиваемых у поставщика услуг доказательств. Например, сообщения в Snapchat следует называть «снэпы». Цель состоит в подготовке простого для восприятия документа, который сразу доносит до читателя суть запроса и при этом обеспечивает необходимую ясность для дальнейших распоряжений суда.

Не следует обозначать ЗВПП как «срочный», кроме действительно чрезвычайных ситуаций. Срок получения электронных доказательств устанавливать не следует, за исключением случаев, когда такой срок определяется фактическими обстоятельствами. К таким обстоятельствам относится, например, истечение срока предварительного заключения. Существует риск того, что при наступлении указанного срока запрашиваемое государство прекратит сбор информации и поместит ЗВПП в архив.

Если запрашиваемое государство сочтет, что установленный срок является нереалистичным, существует вероятность того, что сбор информации не будет проводиться вовсе, поскольку ответственные лица посчитают невозможным предоставление электронных доказательств для целей соответствующего запроса.

В соответствующих случаях ЗВПП следует пометить как «срочный» и представить пояснение относительно того, почему такой ЗВПП должен получить приоритет по отношению к другим. Причинами для этого могут служить серьезность обвинений в рамках расследования/судебного преследования по делам о борьбе с терроризмом и организованной преступностью, а также большое значение электронных доказательств для расследования/судебного преследования или для определения местонахождения других участников Сети, личности которых еще не установлены.

Составитель ЗВПП должен изучить применимый договор о взаимной правовой помощи, чтобы убедиться в том, что срочный запрос может быть передан не по дипломатическим каналам, а напрямую центральному органу запрашиваемого государства, чтобы сэкономить время. Кроме того, следует убедиться в том, что запрашивающее государство может направить ЗВПП с использованием защищенной электронной почты во избежание задержек.

Некоторые государства оказывают ВПП только на основании договора, а другие могут помочь и в отсутствие соответствующих соглашений, на основании принципов взаимности или международной вежливости либо на основании положений своего национального законодательства.

Если запрашиваемому государству для оказания ВПП требуется договор, ЗВПП в отношении электронных доказательств может ссылаться на двусторонние и (или) многосторонние (т. е. региональные, субрегиональные и глобальные) соглашения, как в случаях с ЗВПП в отношении традиционных доказательств.

Некоторые соглашения прямо касаются ВПП в рамках уголовных дел, другие сосредоточены на борьбе с определенными видами правонарушений и в целом включают положения о ВПП. Несмотря на то что в большинстве таких соглашений электронные доказательства прямо не упоминаются, они все равно могут служить правовым основанием для оказания ВПП в отношении электронных доказательств с учетом типов ВПП. Например, в соответствии со ст. 18 Конвенции ООН против транснациональной организованной преступности типы ВПП, которые могут быть запрошены, включают, помимо прочего, «получение свидетельских показаний», «предоставление вещественных доказательств», «проведение обыска и производство выемки» и «оказание любого иного вида помощи, не противоречащего национальному законодательству запрашиваемого государства».

В начале ЗВПП его автор должен кратко обозначить или резюмировать следующую информацию:

— максимально подробные сведения о каждом подозреваемом/обвиняемом по делу (полное имя, дату и место рождения, гражданство, адрес и номер паспорта); также следует отметить, на каком этапе находится расследование или судебное разбирательство;

— требуемые электронные доказательства или метод расследования, а также были ли какие-либо электронные доказательства уже получены без обращения к ВПП (например, посредством направления прямого запроса поставщику услуг).

В ЗВПП требуется лишь сводная информация, а не пространное перечисление всех деталей. Следует привести факты, важные для определения того, какие электронные доказательства запрашиваются, почему эти электронные доказательства необходимы запрашивающему государству, а также каким образом подтверждающие факты удовлетворяют правовому стандарту и прочим законодательным требованиям запрашиваемого государства.

Сводная информация о фактах должна быть изложена ясно, кратко и точно. Лучше всего, если факты будут демонстрировать наличие достаточных для возбуждения дела доказательств того, что каждый из названных обвиняемых совершил означенные уголовные преступления или что было совершено уголовное преступление (если подозреваемые еще не установлены).

В случае расследования/судебного преследования по делам о терроризме такая информация может включать подтверждение того, что террористическая организация определена или запрещена. Это можно установить с помощью национального законодательства, Консолидированного санкционного списка Совета Безопасности ООН.

Кроме того, в ЗВПП необходимо включить достаточное количество подтверждающих сведений и документов, чтобы убедить запрашиваемое государство принять меры к законному принуждению поставщика услуг предоставить требуемые электронные доказательства и создать возможность для принятия таких мер. Это могут быть распоряжения суда о предоставлении информации и (или) соответствующие решения других компетентных национальных органов, если требуется национальный судебный приказ. Составитель ЗВПП должен изучить правовые стандарты запрашиваемого государства, чтобы иметь представление о том, какие подтверждающие сведения и документы необходимо включить.

Чтобы получить ОИА, необходимо установить, что запрашиваемые электронные доказательства являются значимыми и связаны с уголовным расследованием. Недостаточно просто продемонстрировать, что у подозреваемого или обвиняемого есть учетная запись электронной почты или аккаунт в социальной сети; такая учетная запись должна быть связана с расследуемым преступлением. Это самый низкий правовой стандарт, требуемый к соблюдению для всех процедур расследования.

Типы ОИА, которые могут быть доступны для предоставления:

— имя учетной записи или логин пользователя (или абонента);

— полное имя и адрес пользователя;

— номер или номера телефона пользователя;

— адрес электронной почты пользователя;

— дата и время первой регистрации, тип регистрации, копия договора, средства подтверждения личности в момент регистрации, копии документов, представленных пользователем;

— прочая значимая информация, касающаяся личности пользователя/абонента;

— тип услуги, включая идентификатор (номер телефона, IP-адрес, номер SIM-карты, MAC-адрес) и связанное(ые) устройство(а);

— информация профиля (имя пользователя);

— данные о проверке использования услуги, такие как альтернативный адрес электронной почты, предоставленный пользователем/абонентом;

— данные дебетовой или кредитной карты (предоставленные пользователем для целей выставления счетов), включая прочие средства платежа;

— адрес интернет-протокола (IP-адрес), использованный пользователем для регистрации учетной записи или для начала использования услуги иным образом;

— все IP-адреса, использованные пользователем для входа в свою учетную запись;

— время, дата и продолжительность всех сессий;

— прочая информация, касающаяся личности пользователя, включая информацию для выставления счетов (тип и номер кредитных карт, идентификационный номер студента или иная идентифицирующая информация).

3.3. Российский проект конвенции ООН о противодействии использованию информационно-коммуникационных технологий в преступных целях как инструмент международного сотрудничества качественно нового уровня

26 мая 2021 г. в Нью-Йорке в ходе заседания 75-й сессии Генеральной Ассамблеи ООН консенсусом принята российская резолюция 75/282 «О противодействии использованию информационных и коммуникационных технологий (ИКТ) в преступных целях». Документ определяет модальности работы специального комитета для разработки под эгидой ООН универсальной международной конвенции по борьбе с использованием ИКТ в преступных целях (спецкомитета), решение о создании которого было принято в 2019 г. по инициативе России при соавторстве 46 государств.

Предусмотрено, что сессии спецкомитета пройдут поочередно в Нью-Йорке и Вене, начиная с января 2022 г. Орган будет стремиться принимать решения консенсусом, однако предусмотрена возможность голосования, если консенсуса достигнуть не удастся. Проект конвенции должен быть представлен на рассмотрение 78-й сессии Генеральной Ассамблеи ООН в 2023 г.

Консенсусное принятие российского проекта резолюции демонстрирует понимание международным сообществом серьезности угрозы киберпреступности и необходимости выработки универсальных правил борьбы с ней. Запущен открытый, инклюзивный и транспарентный процесс переговоров по проблематике противодействия киберпреступности под эгидой ООН.

Предложенный Россией подход фактически закрепляет *цифровой суверенитет государств над своим информационным пространством* и открывает новую страницу в истории глобального противодействия киберкриминалу. В практическом плане под эгидой Генеральной Ассамблеи ООН создается переговорная площадка для разработки универсальной конвенции по борьбе с киберпреступностью. Таким международным органом станет спецкомитет, в который войдут эксперты из всех стран мира. В свое время аналогичный путь прошли Конвенция ООН против коррупции и Конвенция ООН против транснациональной организованной преступности.

Новая Конвенция видится России и ее единомышленникам как очередной универсальный международный уголовно-правовой инструмент, сфокусированный на преступлениях в сфере использования ИКТ, направленный на борьбу с их противоправным применением и носящий по своему содержанию всеобъемлющий характер. Конвенция должна основываться на принципах уважения государственного суверенитета и невмешательства во внутренние дела государств.

По существу, это первый проект конвенции такого рода на уровне ООН. Конвенция о преступности в сфере компьютерной информации (или Будапештская конвенция) вступила в силу 1 июля 2004 г. К концу 2005 г. ее подписали 38 стран — членов Совета Европы, а также США, Канада, Япония и ЮАР.

Как известно, Россия отказалась от подписания этой Конвенции. Нашей стране не удалось договориться о приемлемых для себя условиях трансграничного доступа к компьютерным системам. Россия оставляла за собой право определиться с участием в Конвенции при условии возможного пересмотра положений п. «b» ст. 32, которые «могут причинить ущерб суверенитету и безопасности государств — участников Конвенции и правам их граждан». Этот пункт гласит, что сторона может без согласия другой стороны «получать через компьютерную систему на своей территории доступ к хранящимся на территории другой стороны компьютерным данным или получить их, если эта сторона имеет законное и добровольное согласие лица, которое имеет законные полномочия раскрывать эти данные этой стороне через такую компьютерную систему».

Кроме того, за прошедшие 20 лет с момента подготовки Будапештской конвенции многие ее положения требуют серьезной доработки и дополнений.

Положено начало субстантивной работе над новой Конвенцией, которая будет учитывать интересы всех без исключения стран и основываться на принципах суверенного равенства сторон и невмешательства во внутренние дела государств. Процесс будет носить динамичный характер и завершится в 2023 г. Для России как инициатора этого процесса консенсусный запуск работы спецкомитета — важный дипломатический успех, результат огромной работы российского МИДа.

Подготовленный проект конвенции имеет ряд преимуществ. Он учитывает современные вызовы и угрозы в сфере международной информационной безопасности (в том числе криминальное использование криптовалюты), вводит новые составы преступлений, совершаемых с использованием ИКТ (распространение фальсифицированной медицинской продукции, оборот наркотиков, вовлечение несовершеннолетних в совершение противоправных деяний, опасных для их жизни и здоровья, и др.). Также проект расширяет сферу международного сотрудничества в вопросах выдачи и оказания правовой помощи по уголовным делам, включая выявление, арест, конфискацию и возврат активов.

27 июля 2021 г. в штаб-квартире ООН в Вене межведомственная российская делегация, возглавляемая заместителем Генерального прокурора РФ, на встрече с и. о. исполнительного директора Управления ООН по наркотикам и преступности Д. Чатчавалитом официально внесла в ООН российский проект конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях.

В ходе работы по проекту конвенции в первую очередь будут обсуждаться следующие важные для следственных и оперативных подразделений вопросы.

Какая информация предоставляется в инициативном порядке? Может ли государство-участник в пределах норм своего внутреннего законодательства направить без предварительного запроса другого государства-участника информацию, полученную в рамках своего собственного расследования, когда, по его мнению, раскрытие такой информации могло бы помочь другому государству-участнику начать или провести расследование? Каковы должны быть условия конфиденциальности работы с информацией?

Как будет осуществляться защита персональных данных? Какие персональные данные могут быть использованы и для каких целей?

Как будут проводиться процедуры направления запросов о взаимной помощи в отсутствие применимых международных соглашений?

Как будут проводиться допросы и иные процессуальные действия с использованием систем видео-конференц-связи или телефонной конференции?

Каковы условия выдачи преступников?

Как будет оперативно обеспечиваться сохранность информации в электронной форме? Какие необходимы сведения, идентифицирующие владельца информации или местоположение устройства ИКТ?

В каких случаях в исполнении запроса об обеспечении сохранности информации может быть отказано? Например, если запрашиваемое государство-участник полагает, что исполнение такого запроса может нанести ущерб его суверенитету, безопасности или другим существенным интересам.

Как будет осуществляться оперативное предоставление сохраненных технических параметров трафика?

Как будет осуществляться взаимная помощь в отношении доступа к хранящимся электронным данным?

Может ли государство-участник попросить другое государство-участника произвести обыск или аналогичные обеспечивающие доступ действия, выемку или аналогичное обеспечение сохранности и раскрытие данных, хранящихся с помощью компьютерной системы, которая находится на территории запрашиваемого государства-участника?

Как будет осуществляться взаимная помощь по сбору технических параметров трафика в режиме реального времени?

Каким путем могут создаваться органы по проведению совместных расследований?

Каким путем могут проводиться специальные методы расследования, такие как электронное наблюдение или другие формы наблюдения и агентурные операции, на своей территории, чтобы доказательства, собранные с помощью таких методов, допускались в суде?

Как будет в надлежащих случаях осуществляться обмен с другими государствами-участниками информацией о конкретных средствах и методах, применяемых для совершения преступлений, охватываемых новой Конвенцией, включая образцы вредоносного программного обеспечения, использование поддельных удостоверений личности, фальшивых, измененных или поддельных документов и других средств для сокрытия противоправной деятельности? Как для этих целей будет использована Международная организация уголовной полиции — Интерпол?

Каковы будут меры по возвращению имущества?

Как будут осуществляться предупреждение и выявление переводов доходов от преступлений, в том числе связанных с оборотом цифровых финансовых активов и цифровой валюты?

Согласование текста глобальной Конвенции и ее открытие для подписания займут не один год. Поэтому Российская Федерация параллельно двигается по пути *укрепления двусторонней базы сотрудничества*.

Прежде всего, речь идет о межправительственных соглашениях, работа над которыми ведется МИДом России.

Кроме того, Федеральным законом от 17 января 1992 г. № 2202-I «О прокуратуре Российской Федерации» Генеральная прокуратура РФ наделена полномочиями по осуществлению прямых связей с компетентными органами других государств и международными организациями, в том числе по заключению с ними межведомственных соглашений и иных договоренностей.

К настоящему времени у России более 90 соглашений с иностранными партнерами. За последнее время заключено четыре из них: с генеральными прокуратурами Бразилии, Португалии, Белиза и Армении. При этом в каждом из четырех соглашений вопросы взаимодействия в области противодействия киберпреступлениям поставлены во главу угла. Эти вопросы также включаются в программы сотрудничества с министерствами юстиции и прокуратурами зарубежных государств, разрабатываемые на краткосрочный период — обычно два-три года.

Кроме того, в декабре 2020 г. тема противодействия киберпреступности стала ключевой на встрече руководителей прокурорских служб стран БРИКС, проведенной под председательством России. Подписан итоговый документ, определивший рамки международного взаимодействия.

ПРИЛОЖЕНИЕ

Конвенция Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях

П р о е к т[1]

Преамбула

Государства — участники настоящей Конвенции,

будучи убеждены в том, что информационное пространство должно строиться в строгом соответствии с основными принципами и нормами международного права, в том числе принципами уважения прав и свобод человека и принципами мирного урегулирования споров,

учитывая, что каждое государство обладает суверенитетом и осуществляет юрисдикцию в отношении информационного пространства в пределах своей территории в соответствии со своим внутренним правом,

будучи обеспокоены серьезностью порождаемых преступлениями в сфере информационно-коммуникационных технологий (ИКТ) проблем и угроз для стабильности и безопасности общества, что подрывает демократические институты, ценности, справедливость и наносит ущерб устойчивому развитию и правопорядку,

будучи обеспокоены также тем, что преступное использование ИКТ создает широкие возможности для осуществления других форм преступной деятельности, включая компьютерные атаки на объекты критически важной инфраструктуры, компьютерный шпионаж, сексуальную эксплуатацию детей в сети Интернет, терроризм, мошенничество, незаконный оборот персональных данных, отмывание денежных средств,

будучи обеспокоены далее возрастающим количеством преступлений в сфере ИКТ, связанных с большими объемами активов, ко-

[1] Передан российской делегацией в специальный комитет ООН 27 июля 2021 г.

торые могут составлять значительную долю ресурсов государств, и ставящих под угрозу социальную, политическую стабильность и устойчивое развитие этих государств,

будучи убеждены в том, что преступления в сфере ИКТ представляют собой транснациональное явление, которое затрагивает общество и экономику всех государств, что обусловливает исключительно важное значение международного сотрудничества в области предупреждения указанных преступлений и борьбы с ними,

будучи убеждены далее в необходимости оказания технической помощи в противодействии преступлениям в сфере ИКТ, которая играет важную роль в расширении возможностей государств в области эффективного предупреждения преступлений и повышения уровня информационной безопасности,

учитывая, что предупреждение и искоренение преступлений в сфере ИКТ — это обязанность всех государств и что для обеспечения эффективности своих усилий в данной области они должны сотрудничать друг с другом при поддержке и участии государственно-частного партнерства, бизнеса, отдельных лиц и групп за пределами публичного сектора, таких как гражданское общество, поскольку общая безопасность всего информационного пространства зависит от усилий каждого государства,

будучи преисполнены решимости более эффективно предупреждать, выявлять и пресекать международные переводы незаконно приобретенных в результате совершения преступлений в сфере ИКТ активов и укреплять международное сотрудничество в принятии мер по возвращению активов,

учитывая также принципы справедливости, равенства перед законом и необходимость содействия формированию в обществе культуры, отвергающей правонарушения в сфере ИКТ,

принимая во внимание резолюцию Генеральной Ассамблеи ООН от 27 декабря 2019 года № 74/274 «Противодействие использованию информационно-коммуникационных технологий в преступных целях», на основании которой учрежден специальный межправительственный комитет экспертов открытого состава для разработки всеобъемлющей международной Конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях,

согласились о нижеследующем:

Глава I
Общие положения

Статья 1. Цели

Целями настоящей Конвенции являются:

содействие принятию и укреплению мер, направленных на эффективное предупреждение преступлений и иных противоправных деяний в сфере ИКТ и борьбу с ними;

предотвращение действий, направленных против конфиденциальности, целостности и доступности ИКТ, и предупреждение злоупотреблений в сфере использования ИКТ путем обеспечения наказуемости деяний, охватываемых настоящей Конвенцией, и предоставления полномочий, достаточных для эффективной борьбы с такими преступлениями и иными противоправными деяниями, путем содействия выявлению и расследованию таких деяний и преследованию за их совершение как на внутригосударственном, так и на международном уровнях и путем разработки договоренностей о международном сотрудничестве;

повышение эффективности и развитие международного сотрудничества, в том числе в контексте подготовки кадров и оказания технической помощи в предупреждении преступлений в сфере ИКТ и борьбе с ними.

Статья 2. Сфера применения

Настоящая Конвенция применяется в соответствии с ее положениями к предупреждению, выявлению, пресечению, расследованию и преследованию за преступления и иные противоправные деяния, признанные таковыми в соответствии со статьями 6—29 настоящей Конвенции, а также осуществлению мер по устранению последствий от совершения таких деяний, включая приостановление операций, связанных с активами, приобретенными в результате совершения какого-либо из преступлений и иных противоправных деяний, признанных таковыми в соответствии с настоящей Конвенцией, арест, конфискацию и возвращение доходов от таких преступлений.

Для целей осуществления настоящей Конвенции, если в ней не предусмотрено иное, не является необходимым, чтобы в результате совершения указанных в ней преступлений и иных противоправных деяний был причинен имущественный вред.

Статья 3. Защита суверенитета

1. Государства-участники осуществляют свои обязательства согласно настоящей Конвенции в соответствии с принципами государственного суверенитета, суверенного равенства государств и невмешательства во внутренние дела других государств.

2. Настоящая Конвенция не наделяет компетентные органы Государства-участника правом осуществлять на территории другого Государства-участника юрисдикцию и функции, которые относятся к исключительной компетенции органов этого другого государства, если иное не предусмотрено в настоящей Конвенции в соответствии с его внутренним законодательством.

Статья 4. Термины и определения

Для целей настоящей Конвенции:

a) «арест имущества» означает временное запрещение передачи, преобразования, отчуждения или передвижения имущества, или временное вступление во владение таким имуществом, или временное осуществление контроля над ним по постановлению суда или другого компетентного органа;

b) «бот-сеть» означает два и более устройства ИКТ, на которые установлена вредоносная программа, управляемая централизованно и скрытно от пользователей;

c) «вредоносная программа» означает программу, объективным свойством которой является несанкционированные модификация, уничтожение, копирование, блокирование информации или нейтрализация средств защиты информации в цифровой форме;

d) «детская порнография» определяется в соответствии с пунктом «c» статьи 2 Факультативного протокола к Конвенции о правах ребенка, касающимся торговли детьми, детской проституции и детской порнографии, от 25 мая 2000 года;

e) «доходы» означают любое имущество, приобретенное или полученное, прямо или косвенно, в результате совершения какого-либо преступления и иного противоправного деяния, предусмотренного настоящей Конвенцией, а также прибыль или другие выгоды, которые получены от таких доходов, от имущества, в которое были превращены или преобразованы такие доходы, или от имущества, к которому были приобщены такие доходы;

f) «информационно-коммуникационные технологии» (ИКТ) означают процессы и методы создания, обработки, распространения информации, а также способы и средства их осуществления;

g) «информационно-телекоммуникационные сети» означают совокупность инженерного оборудования, предназначенного для управления технологическими процессами с применением средств вычислительной техники и телекоммуникаций;

h) «имущество» означает любые активы, материальные и нематериальные, движимые или недвижимые, выраженные в вещах или в правах, включая денежные средства, в том числе находящиеся на банковских счетах, цифровые финансовые активы, цифровую валюту, включая криптовалюту, а также юридические документы или акты, подтверждающие право на такие активы или на их часть;

i) «информация» означает любые сведения (сообщения, данные), независимо от формы их представления;

j) «конфискация» означает принудительное безвозмездное изъятие имущества на основании постановления суда или другого компетентного органа;

k) «компьютерная атака» означает целенаправленное воздействие программных и (или) программно-аппаратных средств на информационные системы или информационно-телекоммуникационные сети в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации;

l) «цифровая информация» означает сведения (данные), независимо от формы и характеристик, содержащиеся и обрабатываемые в информационно-телекоммуникационных устройствах, системах и сетях;

m) «критическая информационная инфраструктура» означает совокупность объектов критической информационной инфраструктуры, а также сетей электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры между собой;

n) «объекты критической инфраструктуры» означают информационные системы и информационно-коммуникационные сети государственных органов, а также информационные системы и автоматизированные системы управления технологическими процессами, функционирующие в сфере оборонной промышленности,

здравоохранения, образования, транспорта, связи, энергетики, в кредитно-финансовой сфере, атомной и других важных сферах жизнедеятельности государства и общества;

o) «поставщик услуг» означает:

i) любую государственную или частную организацию, которая обеспечивает пользователям ее услуг возможность обмена информацией посредством использования ИКТ, или

ii) любую другую организацию, которая осуществляет обработку или хранение информации в электронной форме от имени организации, упомянутой в подпункте (i), или пользователей услуг такой организации;

p) «технические параметры трафика» означают любую информацию в электронной форме (за исключением содержания передаваемых данных), связанную с передачей данных с использованием ИКТ и указывающую, в частности, на источник передачи данных, пункт назначения, маршрут, время, дату, размер, продолжительность, тип соответствующего сетевого сервиса;

q) «устройство ИКТ» означает совокупность (комплекс) технических средств, использующуюся/предназначенную для автоматизированной обработки, хранения и передачи информации в электронной форме;

r) «электронное доказательство» означает любую доказательную информацию, хранимую или передаваемую в цифровой форме (на электронном носителе информации).

Понятие «существенный ущерб» определяется в соответствии с внутренним законодательством запрашиваемого Государства-участника.

Глава II
Криминализация, уголовное производство и правоохранительная деятельность

Раздел 1
Установление ответственности

Статья 5. Установление ответственности

Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления, согласно его внутреннему законодательству, деяний, предусмотренных как минимум статьями 6, 7, 9—12, 14—17, 19—20, 22—26, 28 настоящей Конвенции, применяя при этом такие уголовные и иные санкции, включая лишение свободы, которые учитывают степень общественной опасности конкретного деяния и размер причиненного ущерба.

Статья 6. Неправомерный доступ к цифровой информации

Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления, согласно его внутреннему законодательству, умышленного, неправомерного доступа к цифровой информации, повлекшего ее уничтожение, блокирование, модификацию либо копирование.

Статья 7. Неправомерный перехват

Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления, согласно его внутреннему законодательству, умышленного перехвата цифровой информации, осуществляемого без соответствующих прав и (или) с нарушением установленных норм, в том числе с использованием технических средств перехвата технических параметров трафика и данных, обрабатываемых с использованием ИКТ и не предназначенных для общего пользования.

Статья 8. Неправомерное воздействие на цифровую информацию

Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления или иного противоправного деяния, согласно его внутреннему законодательству, умышленного, неправомерного воздействия на цифровую информацию путем ее повреждения, удаления, изменения, блокирования, модификации либо копирования информации в цифровой форме.

Статья 9. Нарушение функционирования информационно-коммуникационных сетей

Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления, согласно его внутреннему законодательству, умышленного, неправомерного действия, направленного на нарушение

функционирования информационно-коммуникационных сетей, повлекшего тяжкие последствия или создавшего угрозу их наступления.

Статья 10. Создание, использование и распространение вредоносных программ

1. Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления, согласно его внутреннему законодательству, умышленного создания, в том числе адаптирования, использования и распространения вредоносных программ, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования, распространения цифровой информации или нейтрализации средств ее защиты, за исключением случаев правомерного проведения исследований.

2. Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления или иного противоправного деяния, согласно его внутреннему законодательству, создания или использования бот-сети для целей совершения какого-либо из деяний, предусмотренных положениями статей 6—12, 14 настоящей Конвенции.

Статья 11. Неправомерное воздействие на критическую информационную инфраструктуру

1. Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления, согласно его внутреннему законодательству, умышленного создания, распространения и (или) использования компьютерных программ либо иной цифровой информации, заведомо предназначенных для неправомерного воздействия на критическую информационную инфраструктуру, в том числе для уничтожения, блокирования, модификации, копирования информации, содержащейся в ней, или нейтрализации средств защиты.

2. Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления, согласно его внутреннему законодательству, нарушения правил эксплуатации средств хранения, обработки и передачи охраняемой цифровой информации, содержащейся в критической информационной инфраструктуре, или информационных

систем, информационно-коммуникационных сетей, относящихся к критической информационной инфраструктуре, либо правил доступа к ним, если оно повлекло причинение вреда критической информационной инфраструктуре.

Статья 12. Несанкционированный доступ к персональным данным

Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания, согласно его внутреннему законодательству, в качестве преступления несанкционированного доступа к персональным данным в целях их уничтожения, изменения, копирования, распространения.

Статья 13. Незаконный оборот устройств

Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления или иного противоправного деяния, согласно его внутреннему законодательству, незаконного производства, продажи, приобретения для использования, импорта, экспорта или иных форм предоставления в пользование устройств, разработанных или адаптированных прежде всего для целей совершения какого-либо из преступлений, предусмотренных положениями статей 6—12 настоящей Конвенции.

Положения настоящей статьи не распространяются на случаи, когда производство, продажа, приобретение для использования, импорт, экспорт или иные формы предоставления в пользование устройств связаны, например, с разрешенным испытанием или защитой компьютерной системы.

Статья 14. Хищение с использованием ИКТ

1. Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления, согласно его внутреннему законодательству, хищения имущества либо незаконного приобретения права на него, в том числе посредством мошенничества, путем уничтожения, блокирования, модификации либо копирования цифровой информации или иного вмешательства в функционирование ИКТ.

2. Каждое Государство-участник может оставить за собой право считать хищение имущества либо незаконное приобретение права на него, в том числе посредством мошенничества, с использо-

ванием ИКТ признаком, отягчающим наказание при совершении хищения в формах, определенных внутренним законодательством.

Статья 15. Преступления, связанные с изготовлением и оборотом материалов или предметов с порнографическими изображениями несовершеннолетних, совершенные с использованием ИКТ

1. Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления, согласно его внутреннему законодательству, совершения умышленно и неправомерно следующих деяний:

a) производство детской порнографической продукции в целях распространения через информационно-коммуникационные сети, включая сеть Интернет;

b) предложение или предоставление в пользование детской порнографии через информационно-коммуникационные сети, включая сеть Интернет;

c) распространение, передача, публичная демонстрация или рекламирование детской порнографии с использованием информационно-коммуникационных сетей, включая сеть Интернет;

d) приобретение детской порнографии посредством использования ИКТ для себя или для другого лица;

e) владение детской порнографией, находящейся в компьютерной системе или на электронно-цифровых носителях информации.

2. Для целей пункта 1 настоящей статьи в понятие «детская порнография» включаются порнографические материалы, изображающие:

a) участие несовершеннолетнего лица в откровенных сексуальных действиях;

b) участие лица, кажущегося несовершеннолетним, в откровенных сексуальных действиях;

c) реалистические изображения несовершеннолетнего лица, участвующего в откровенных сексуальных действиях.

Для целей настоящей статьи термин «несовершеннолетние» означает любое лицо, не достигшее 18-летнего возраста. Однако любая Сторона может устанавливать и более низкие возрастные пределы, но не ниже 16 лет.

Статья 16. Склонение к самоубийству или доведение до его совершения

Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления, согласно его внутреннему законодательству, склонения к самоубийству или доведения до самоубийства, в том числе несовершеннолетних, совершенных посредством оказания психологического и иных видов воздействия в информационно-телекоммуникационных сетях, включая сеть Интернет.

Статья 17. Преступления, связанные с вовлечением несовершеннолетнего в совершение противоправных действий, опасных для его жизни и здоровья

Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления, согласно его внутреннему законодательству, вовлечения несовершеннолетнего посредством использования ИКТ в совершение противоправных деяний, представляющих опасность для его жизни, за исключением действий, предусмотренных статьей 16 настоящей Конвенции.

Статья 18. Создание и использование цифровой информации для введения пользователя в заблуждение

1. Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления или иного противоправного деяния, согласно его внутреннему законодательству, умышленного противоправного создания и использования цифровой информации, сходной до степени смешения с уже известной пользователю и вызывающей доверие информацией, повлекших причинение существенного ущерба.

2. Каждое Государство-участник может оставить за собой право считать такие деяния преступными, если они совершены в совокупности с иными преступлениями, предусмотренными внутренним законодательством такого Государства-участника, или содержали умысел совершения указанных преступлений.

Статья 19. Подстрекательство к подрывной или вооруженной деятельности

Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления, согласно его внутреннему законодательству, совершенных с использованием ИКТ призывов к проведению подрывных или вооруженных действий, направленных на насильственное изменение государственного строя другого государства.

Статья 20. Преступления, связанные с террористической деятельностью

Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления, согласно его внутреннему законодательству, совершенных с использованием ИКТ призывов к осуществлению террористической деятельности, склонения, вербовки или иного вовлечения в нее, пропаганды и оправдания терроризма, сбора или предоставления средств для целей его финансирования.

Статья 21. Преступления, связанные с экстремистской деятельностью

1. Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления или иного противоправного деяния, согласно его внутреннему законодательству, распространения материалов, содержащих призывы к совершению противоправных деяний по мотивам политической, идеологической, социальной, расовой, национальной или религиозной ненависти и вражды, пропаганды или оправдания таких деяний, либо обеспечения доступа к ним, совершенных с использованием ИКТ.

2. Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления или иного противоправного деяния, согласно его внутреннему законодательству, унижения лица или группы лиц по признакам расы, национальности, языка, происхождения, отношения к религии, совершенного с использованием ИКТ.

Статья 22. Преступления, связанные с распространением наркотических средств и психотропных веществ

Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве

преступления, согласно его внутреннему законодательству, совершенного умышленно, посредством использования ИКТ, незаконного оборота наркотических средств и психотропных веществ, а также материалов, необходимых для их изготовления.

Статья 23. Преступления, связанные с незаконным оборотом оружия

Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления, согласно его внутреннему законодательству, совершенного умышленно, посредством использования ИКТ, незаконного оборота оружия, боеприпасов, взрывных устройств и взрывчатых веществ.

Статья 24. Реабилитация нацизма, оправдание геноцида или преступлений против мира и человечности

Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления, согласно его внутреннему законодательству, совершенного с использованием ИКТ, умышленного распространения материалов, в которых отрицаются факты, одобряются или оправдываются действия, являющиеся геноцидом или преступлениями против мира и человечности, установленные приговором Международного военного трибунала, образованного в соответствии с Лондонским соглашением от 8 августа 1945 года.

Статья 25. Незаконное распространение фальсифицированных лекарственных средств и медицинских изделий

Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления, согласно его внутреннему законодательству, совершенного умышленно, посредством использования ИКТ, незаконного распространения фальсифицированных лекарственных средств и медицинских изделий.

Статья 26. Использование ИКТ для совершения деяний, признанных преступлениями в соответствии с международным правом

1. Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в каче-

стве преступления, согласно его внутреннему законодательству, использования ИКТ с целью совершения какого-либо деяния, представляющего собой преступление, охватываемое каким-либо международным договором из перечисленных в приложении к настоящей Конвенции.

2. При сдаче на хранение своих ратификационных грамот или документов о принятии, утверждении или присоединении государство, не являющееся участником какого-либо из договоров, перечисленных в приложении к настоящей Конвенции, может заявить, что при применении настоящей Конвенции к этому Государству-участнику считается, что этот договор не включен в упомянутое приложение. Такое заявление перестает действовать, как только этот договор вступает в силу для данного Государства-участника, которое уведомляет об этом факте депозитария.

3. Когда Государство-участник перестает быть стороной какого-либо из договоров, перечисленных в приложении к настоящей Конвенции, оно может сделать заявление в отношении этого договора (договоров), как это предусматривается в пункте 2 настоящей статьи.

Статья 27. Нарушение авторских и смежных прав с использованием ИКТ

Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления или иного противоправного деяния, согласно его внутреннему законодательству, нарушения авторских и смежных прав, как они определены в законодательстве этого Государства-участника, когда такие деяния совершаются умышленно, с использованием ИКТ, включая незаконное использование программ для компьютерных систем и баз данных, являющихся объектами авторского права, и присвоение авторства.

Статья 28. Соучастие в преступлении, приготовление к преступлению и покушение на преступление

1. Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления, в соответствии со своим внутренним законодательством, приготовления и покушения на какое-либо преступление, признанное таковым в соответствии с положениями настоящей Конвенции.

2. Каждое Государство-участник рассматривает возможность принятия таких законодательных и иных мер, которые необходимы для признания в качестве преступления, в соответствии со своим внутренним законодательством, изготовления или приспособления лицом орудий и иных средств совершения преступления, вербовки соучастников преступления, сговора на совершение преступления либо иного умышленного создания условий для совершения преступления, предусмотренного настоящей Конвенцией, если при этом преступление не было доведено до конца по не зависящим от этого лица обстоятельствам.

3. Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы, согласно его внутреннему законодательству, для установления ответственности, наряду с непосредственными исполнителями какого-либо преступления, признанного таковым в соответствии с настоящей Конвенцией, в отношении участвующих в его совершении организатора, подстрекателя или пособника, а также усиления ответственности за групповые преступления, включая организованные группы и преступные сообщества.

Статья 29. Иные противоправные деяния

Настоящая Конвенция не является препятствием для признания Государством-участником в качестве преступления любого другого противоправного деяния, совершенного умышленно, с использованием ИКТ и повлекшего существенный ущерб.

Статья 30. Ответственность юридических лиц

1. Каждое Государство-участник принимает такие законодательные и иные правовые меры, которые необходимы для обеспечения возможности привлечения к ответственности юридических лиц в связи с преступлениями и иными противоправными деяниями, признанными в качестве таковых в соответствии с настоящей Конвенцией, если эти деяния совершены в их интересах любым физическим лицом, действующим в личном качестве или в качестве члена органа соответствующего юридического лица, занимающего в данном юридическом лице руководящую должность на основании:

a) полномочий представлять данное юридическое лицо;

b) права принимать решения от имени этого юридического лица;

c) права осуществлять контроль внутри этого юридического лица.

2. В дополнение к случаям, предусмотренным пунктом 1 настоящей статьи, каждое Государство-участник принимает меры, необходимые для обеспечения возможности возложения ответственности на юридическое лицо в случаях, когда отсутствие руководства или контроля со стороны физического лица, упомянутого в пункте 1, делает возможным совершение преступления или иного противоправного деяния, предусмотренного положениями настоящей Конвенции, в пользу этого юридического лица физическим лицом, действующим на основании данных ему полномочий.

3. В зависимости от правовых принципов Государства-участника ответственность юридического лица может быть уголовной, гражданско-правовой или административной. Государство-участник обеспечивает применение в отношении юридических лиц, привлекаемых к ответственности, эффективных, соразмерных и оказывающих сдерживающее воздействие санкций, включая финансовые.

4. Привлечение к ответственности юридических лиц не исключает привлечения к ответственности физических лиц, совершивших преступление и иное противоправное деяние.

Раздел 2
Уголовное судопроизводство и правоохранительная деятельность

Статья 31. Сфера применения процессуальных норм

1. Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для установления полномочий и процедур, предусмотренных положениями настоящего раздела, в целях предупреждения, выявления, пресечения, раскрытия и расследования преступлений и иных противоправных деяний и осуществления судебного разбирательства в связи с ними.

2. За исключением случаев, когда положениями статьи 33 настоящей Конвенции предусматривается иное, каждое Государство-участник применяет полномочия и процедуры, упомянутые в пункте 1 настоящей статьи, в отношении:

a) преступлений и иных противоправных деяний, предусмотренных статьями 6—29 настоящей Конвенции;

b) других преступлений и иных противоправных деяний, совершенных с использованием ИКТ;

c) сбора доказательств, в том числе электронных, совершения преступлений и иных противоправных деяний.

3. a) Каждое Государство-участник может сделать оговорку о сохранении за собой права применять меры, предусмотренные статьей 38 настоящей Конвенции, только в отношении преступлений или категорий преступлений, указанных в этой оговорке, при условии, что круг таких преступлений или категорий преступлений не более ограничен, чем круг преступлений, к которым оно применяет меры, предусмотренные статьей 33 настоящей Конвенции. Каждое Государство-участник рассматривает возможность ограничения сферы действия такой оговорки с целью максимально широкого применения мер, предусмотренных положением статьи 38 настоящей Конвенции;

b) в том случае, когда Государство-участник ввиду ограничений, предусмотренных внутренним законодательством, действующим на момент принятия настоящей Конвенции, не имеет возможности применить меры, предусмотренные статьями 33 и 38 настоящей Конвенции, к информации, передаваемой по информационной системе поставщика услуг, которая:

i) используется для обслуживания отдельной группы пользователей и

ii) не использует информационно-телекоммуникационную сеть, а также не соединена ни с какими другими информационными системами,

это Государство-участник может сохранить за собой право не применять указанные меры к такой передаче информации.

Статья 32. Условия и гарантии

1. Каждое Государство-участник обеспечивает, чтобы установление, исполнение и применение полномочий и процедур, предусмотренных настоящим разделом, осуществлялись в соответствии с условиями и гарантиями, предусмотренными нормами ее внутреннего законодательства, обеспечивающими надлежащую защиту прав и свобод человека, включая права, вытекающие из обязательств, которые Государство-участник взяло на себя по Международному пакту о гражданских и политических правах от 16 декабря 1966 года и по другим применимым международным договорам по правам человека.

2. Такие условия и гарантии с учетом характера полномочий и процедур включают, среди прочего, судебный или иной независимый надзор, основания правомочности применения, ограничения сферы и сроков действия таких полномочий или процедур.

3. В той мере, в какой это соответствует публичным интересам, в частности осуществлению правосудия, Государство-участник рассматривает влияние предусмотренных данным разделом полномочий и процедур на права, законные интересы и ответственность третьих лиц.

Статья 33. Сбор информации, передаваемой с использованием ИКТ

1. Каждое Государство-участник принимает такие законодательные и иные меры в целях противодействия преступлениям, предусмотренным настоящей Конвенцией и признанным таковыми в соответствии с его внутренним законодательством, какие могут быть необходимы для того, чтобы наделить его компетентные органы полномочиями:

a) собирать или записывать с применением технических средств информацию, передаваемую с использованием ИКТ, на территории этого Государства-участника, и

b) обязать поставщика услуг в пределах имеющихся у него технических возможностей:

i) собирать или записывать с использованием технических средств на территории этого Государства-участника информацию в электронной форме, включающую данные о содержании сообщений, передаваемую с использованием ИКТ, или

ii) сотрудничать с компетентными органами этого Государства-участника и помогать им в сборе или записи в режиме реального времени информации в электронной форме, включающей данные о содержании сообщений, передаваемой с использованием ИКТ, на территории этого Государства-участника.

2. Если какое-либо Государство-участник в силу устоявшихся принципов его системы внутреннего права не может принять меры, предусмотренные в пункте 1(a) настоящей статьи, то вместо этого оно может принять законодательные и иные меры, какие могут быть необходимы для обеспечения сбора или записи в режиме реального времени информации в электронной форме, включающей данные о содержании сообщений, передаваемой с использованием ИКТ на его территории, путем применения технических средств на этой территории.

3. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут быть необходимы для того, чтобы обязать поставщика услуг соблюдать конфиденциальность факта осуществления любых полномочий и действий, предусмотренных в настоящей статье, и любой информации об этом.

4. Полномочия и процедуры, упомянутые в настоящей статье, устанавливаются в соответствии с положениями статей 31 и 32 настоящей Конвенции.

Статья 34. Оперативное обеспечение сохранности накопленной информации в электронной форме

1. Каждое Государство-участник принимает такие законодательные и иные меры, которые могут потребоваться для того, чтобы его компетентные органы имели возможность отдавать соответствующие распоряжения или указания или схожим образом оперативно обеспечивать сохранность конкретной электронно-цифровой информации, включая технические параметры трафика, в частности в случаях, когда имеются основания полагать, что эти данные особенно подвержены риску уничтожения, блокирования, копирования или модификации, в том числе в результате истечения срока давности их хранения, установленного внутренним законодательством или правилами предоставления услуг провайдера.

2. Если Государство-участник реализует положения пункта 1 настоящей статьи посредством дачи распоряжения какому-либо лицу (в том числе юридическому) об обеспечении сохранности конкретной хранимой информации, находящейся во владении или под контролем этого лица, то это Государство-участник принимает такие законодательные и иные правовые меры, какие могут потребоваться для того, чтобы обязать это лицо хранить эту информацию и обеспечивать ее целостность в течение необходимого периода времени, но не превышающего такого срока, установленного внутренним законодательством этого Государства-участника, с тем чтобы компетентные органы могли добиться раскрытия этих данных. Государство-участник может предусмотреть возможность продления срока действия такого распоряжения.

3. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут быть необходимы для того, что-

бы обязать лицо, на которое возложена обязанность по обеспечению сохранности информации, соблюдать конфиденциальность выполнения таких процедур в течение срока, предусмотренного его внутренним законодательством.

4. Полномочия и процедуры, упомянутые в настоящей статье, устанавливаются в соответствии с положениями статей 31 и 32 настоящей Конвенции.

Статья 35. Оперативное обеспечение сохранности и частичное раскрытие данных о технических параметрах трафика

1. Каждое Государство-участник принимает в отношении технических параметров трафика, сохранность которых должна быть обеспечена в соответствии с положениями статьи 34 настоящей Конвенции, такие законодательные и иные меры, какие могут быть необходимы для того, чтобы:

a) гарантировать, чтобы такое оперативное обеспечение сохранности технических параметров трафика было возможным независимо от того, сколько поставщиков услуг были вовлечены в передачу данной информации; и

b) гарантировать оперативное раскрытие компетентным органам этого Государства-участника достаточного количества технических параметров трафика, которое позволит соответствующему Государству-участнику идентифицировать поставщиков услуг и путь, которым передавалась указанная информация.

2. Полномочия и процедуры, упомянутые в настоящей статье, устанавливаются в соответствии с положениями статей 31 и 32 настоящей Конвенции.

Статья 36. Распоряжение о предоставлении информации

1. В целях, предусмотренных пунктом 1 статьи 31 настоящей Конвенции, каждое Государство-участник принимает такие законодательные и иные меры, какие могут быть необходимы для того, чтобы предоставить своим компетентным органам полномочия отдавать распоряжения:

a) лицу на территории этого Государства-участника о предоставлении конкретной электронно-цифровой информации, находящейся во владении или под контролем этого лица;

b) поставщику услуг, предлагающему свои услуги на территории этого Государства-участника, о предоставлении находящихся во владении или под контролем этого поставщика услуг сведений о его абонентах.

2. Полномочия и процедуры, упомянутые в настоящей статье, устанавливаются в соответствии с положениями статей 31 и 32 настоящей Конвенции.

3. Для целей настоящей статьи термин «сведения об абонентах» означает любую имеющуюся у поставщика услуг информацию о его абонентах, кроме технических параметров трафика или содержания информации, с помощью которых можно определить:

a) вид используемой информационно-коммуникационной услуги, принятые с этой целью меры технического обеспечения и период оказания услуги;

b) личность пользователя, его почтовый или иные адреса, номера телефонов и других средств связи, включая IP-адреса, сведения о выставленных ему счетах и произведенных им платежах в рамках соглашения или договора на обслуживание;

c) сведения о месте установки информационно-коммуникационного оборудования, имеющего отношение к соглашению или договору на его обслуживание.

Статья 37. Обыск и выемка информации, хранимой или обрабатываемой в электронной форме

1. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться для предоставления его компетентным органам полномочий на обыск в целях получения доступа к находящимся на территории этого Государства-участника или под его юрисдикцией:

a) устройствам ИКТ и хранящейся на них информации и

b) носителям информации, на которых может храниться искомая электронно-цифровая информация.

2. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут быть необходимы для обеспечения того, чтобы в случае, когда его компетентные органы в ходе обыска, производимого в соответствии с положениями пункта 1(a) настоящей статьи, выясняют, что искомая информация хранится на другом устройстве ИКТ на территории этого Государства-участника, такие органы имели возможность оперативно произвести обыск в целях получения доступа к этому другому устройству ИКТ или содержащимся в нем данным.

3. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут быть необходимы для предоставления его компетентным органам полномочий производить выемку на территории либо под юрисдикцией Государства-участника информации в электронной форме или иным аналогичным образом обеспечивать ее сохранность. Эти меры должны включать, в частности, предоставление следующих полномочий:

a) производить выемку устройств ИКТ, используемых для хранения информации, либо иным образом обеспечивать их сохранность;

b) изготавливать и сохранять копии соответствующей информации в электронно-цифровой форме;

c) обеспечивать целостность относящейся к делу хранимой информации;

d) изымать информацию, хранящуюся или обрабатываемую в электронно-цифровой форме на устройстве ИКТ.

4. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут быть необходимы для предоставления его компетентным органам полномочий привлекать в порядке, установленном его внутренним законодательством, любое лицо, обладающее специальными знаниями о функционировании соответствующей информационной системы, информационно-телекоммуникационной сети или их частей или применяемых мерах защиты информации, для предоставления необходимых сведений и (или) оказания содействия в осуществлении действий, предусмотренных пунктами 1—3 настоящей статьи.

5. Полномочия и процедуры, упомянутые в настоящей статье, устанавливаются в соответствии с положениями статей 31 и 32 настоящей Конвенции.

Статья 38. Сбор в режиме реального времени технических параметров трафика

1. Каждое Государство-участник принимает такие законодательные и иные меры, которые могут быть необходимы для предоставления его компетентным органам полномочий:

a) собирать или записывать с применением технических средств технические параметры трафика, передаваемого с использованием ИКТ, на территории этого Государства-участника, и

b) обязать поставщиков услуг в пределах имеющихся у них технических возможностей:

i) собирать или записывать с применением технических средств на территории этого Государства-участника технические параметры трафика или

ii) сотрудничать с компетентными органами этого Государства-участника и помогать им собирать или записывать в режиме реального времени технические параметры трафика, связанные с конкретной информацией, на территории этого Государства-участника.

2. Если какое-либо Государство-участник в силу устоявшихся принципов его системы внутреннего законодательства не может принять меры, предусмотренные в пункте 1(a) настоящей статьи, то вместо этого оно может принять законодательные и иные меры, какие могут быть необходимы для обеспечения сбора или записи в режиме реального времени технических параметров трафика на его территории путем применения технических средств на этой территории.

3. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут быть необходимы для того, чтобы обязать поставщика услуг соблюдать конфиденциальность факта осуществления любых полномочий, предусмотренных в настоящей статье, и любой информации об этом.

4. Полномочия и процедуры, упомянутые в настоящей статье, устанавливаются в соответствии с положениями статей 31 и 32 настоящей Конвенции.

Статья 39. Юрисдикция

1. Каждое Государство-участник принимает такие меры, какие могут потребоваться, с тем чтобы установить свою юрисдикцию в отношении преступлений и иных противоправных деяний, признанных таковыми в соответствии с настоящей Конвенцией, когда они совершены:

a) на территории этого Государства-участника или

b) борту судна, которое несло флаг этого Государства-участника в момент совершения деяния, или воздушного судна, которое зарегистрировано в соответствии с законодательством этого Государства-участника в такой момент.

2. При условии соблюдения статьи 3 настоящей Конвенции Государство-участник может также установить свою юрисдикцию в

отношении любого такого преступления и иного противоправного деяния, когда:

a) деяние совершено против гражданина этого Государства-участника, лица без гражданства, постоянно проживающего на его территории, юридического лица, учрежденного или имеющего постоянное представительство на его территории, государственного или правительственного объекта, включая помещения дипломатического представительства и консульского учреждения этого Государства-участника; или

b) деяние совершено гражданином этого Государства-участника или лицом без гражданства, которое обычно проживает на его территории; или

c) деяние совершено против этого Государства-участника; или

d) деяние совершено полностью или частично за пределами территории Государства-участника, но его последствия составляют на его территории преступление или приводят к совершению преступления.

3. Для целей статьи 47 настоящей Конвенции каждое Государство-участник принимает такие меры, какие могут потребоваться, с тем чтобы установить свою юрисдикцию в отношении преступлений, признанных таковыми в соответствии с настоящей Конвенцией, когда лицо, подозреваемое в совершении преступления, находится на его территории и оно не выдает такое лицо на том основании, что это лицо является его гражданином либо лицом, которому этим Государством-участником предоставлен статус беженца.

4. Каждое Государство-участник, на территории которого находится лицо, подозреваемое в совершении преступления, и которое не выдает его, обязано в случаях, предусмотренных в пунктах 1 и 2 настоящей статьи, без каких бы то ни было исключений и независимо от того, совершено ли оно на территории этого Государства-участника, без излишних задержек передать дело своим компетентным органам для целей преследования путем проведения разбирательства в соответствии с законодательством этого Государства.

5. Если Государство-участник, осуществляющее свою юрисдикцию, согласно пункту 1 или 2 настоящей статьи, получает уведомление или иным образом узнает о том, что любые другие государства-участники осуществляют расследование, уголовное преследование или судебное разбирательство в связи с тем же деянием,

компетентные органы этих государств-участников проводят в надлежащих случаях консультации друг с другом с целью координации своих действий.

6. Без ущерба для норм общего международного права настоящая Конвенция не исключает осуществления любой уголовной и административной юрисдикции, установленной Государством-участником в соответствии со своим внутренним законодательством.

Глава III
Меры по противодействию преступлениям и иным противоправным деяниям в информационном пространстве

Статья 40. Политика и практика предупреждения преступлений и иных противоправных деяний в сфере использования ИКТ и борьбы с ними

1. Каждое Государство-участник в соответствии с основополагающими принципами своей правовой системы разрабатывает и осуществляет или проводит эффективную и скоординированную политику противодействия преступлениям и иным противоправным деяниям в сфере использования ИКТ.

2. Каждое Государство-участник стремится разрабатывать и поощрять эффективные виды практики, направленные на предупреждение преступлений и иных противоправных деяний в сфере использования ИКТ.

3. Государства-участники в надлежащих случаях в соответствии с основополагающими принципами своих правовых систем взаимодействуют друг с другом и с соответствующими международными и региональными организациями в разработке мер, указанных в настоящей статье, и содействии их осуществлению.

Статья 41. Органы по предупреждению преступлений и иных противоправных деяний в сфере использования ИКТ и борьбе с ними

1. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут быть необходимы для того, чтобы определить органы, ответственные за осуществление деятельности по предупреждению преступлений и иных противоправных деяний в сфере использования ИКТ и борьбе с ними, и порядок взаимодействия этих органов между собой.

2. Каждое Государство-участник сообщает Генеральному секретарю Организации Объединенных Наций наименование и адрес органа или органов, которые могут оказывать другим государствам-участникам содействие в разработке и осуществлении конкретных мер по предупреждению преступлений и иных противоправных деяний в сфере использования ИКТ.

Статья 42. Частный сектор

1. Каждое Государство-участник принимает меры в соответствии с основополагающими принципами своего внутреннего законодательства по предупреждению преступлений и иных противоправных деяний в сфере использования ИКТ в частном секторе, усилению стандартов информационной безопасности в частном секторе и в надлежащих случаях установлению и применению эффективных, соразмерных и оказывающих сдерживающее воздействие гражданско-правовых, административных или уголовных санкций за несоблюдение таких мер.

2. Меры, направленные на достижение этих целей, могут включать среди прочего следующее:

a) содействие сотрудничеству между правоохранительными органами Государства-участника и соответствующими частными организациями данного Государства-участника;

b) содействие разработке стандартов и процедур, предназначенных для обеспечения информационной безопасности;

c) содействие в обучении представителей правоохранительных, следственных, судебных органов и органов прокуратуры в сфере использования ИКТ.

Статья 43. Принципы и стандарты поведения частных организаций, предоставляющих информационно-телекоммуникационные услуги

1. Каждая частная организация (или их объединение), предоставляющая информационно-телекоммуникационные услуги, находящаяся на территории Государства-участника, принимает надлежащие меры, в пределах своих возможностей и в соответствии с нормами внутреннего права этого государства, для содействия формулированию и реализации принципов и стандартов функционирования международного информационного пространства на основе соблюдения прав человека, закрепленных в основополагающих документах Организации Объединенных Наций.

2. Меры, направленные на достижение этих целей, могут включать среди прочего следующее:

a) сотрудничество между частными организациями, предоставляющими информационно-телекоммуникационные услуги, и их объединениями;

b) сотрудничество в разработке принципов и стандартов, предназначенных для создания подходящей среды для цивилизованного общества как неотъемлемой части международного информационного пространства.

Статья 44. Повышение информированности общества в сфере предупреждения информационной преступности

1. Каждое Государство-участник принимает надлежащие меры в пределах своих возможностей и в соответствии с основополагающими принципами своего внутреннего права для содействия активному участию общественных организаций в предупреждении преступлений и иных противоправных деяний в сфере использования ИКТ и для углубления понимания обществом факта существования, причин и опасного характера этих преступлений, а также создаваемых ими угроз. Это участие следует укреплять с помощью таких мер, как:

a) обеспечение для населения эффективного доступа к информации;

b) проведение мероприятий по информированию населения, способствующих созданию атмосферы нетерпимости в отношении преступлений и иных противоправных деяний в сфере использования ИКТ, а также с целью распространения передового опыта;

c) осуществление программ публичного образования в области обеспечения безопасности ИКТ.

2. Каждое Государство-участник принимает надлежащие меры для обеспечения того, чтобы соответствующие органы по противодействию преступлениям и иным противоправным деяниям в сфере использования ИКТ, о которых говорится в настоящей Конвенции, были известны населению, и обеспечивает доступ к таким органам для предоставления им сообщений о любых случаях, которые могут рассматриваться в качестве преступлений и иных противоправных деяний в соответствии с настоящей Конвенцией.

Статья 45. Меры по защите свидетелей

Каждое Государство-участник рассматривает возможность принятия таких законодательных мер, которые могут быть необходимы для обеспечения эффективной защиты:

a) лиц, которые добросовестно и на разумных основаниях предоставляют информацию, касающуюся противоправных деяний, предусмотренных статьями 6—28 настоящей Конвенции, или иным образом сотрудничают со следственными или судебными органами;

b) свидетелей, дающих показания в отношении противоправных деяний, предусмотренных статьями 6—28 настоящей Конвенции, а также потерпевших;

c) при необходимости членов семей лиц, указанных в пунктах «a» и «b» настоящей статьи.

Глава IV
Международное сотрудничество

Раздел 1
Выдача, взаимная правовая помощь и сотрудничество между правоохранительными органами

Статья 46. Общие принципы международного сотрудничества

1. Государства-участники осуществляют максимально широкое сотрудничество в соответствии с положениями настоящей главы и путем применения других международных договоров о международном сотрудничестве по уголовным делам, согласованных договоренностей, основанных на принципе взаимности, а также норм внутреннего законодательства в целях предупреждения, пресечения, выявления, раскрытия и расследования преступлений в сфере использования ИКТ.

2. Когда применительно к вопросам международного сотрудничества требуется соблюдение принципа обоюдного признания соответствующего деяния преступлением, этот принцип считается соблюденным независимо от того, включает ли законодательство запрашиваемого Государства-участника соответствующее деяние в ту же категорию преступлений, или оно описывает его с помощью таких же терминов, как запрашивающее Государство-участник, если деяние, образующее состав преступления, в связи с которым запрашивается помощь, признано уголовно наказуемым в соответствии с законодательством обоих государств-участников.

3. Когда это целесообразно и соответствует их внутренней правовой системе, государства-участники оказывают друг другу содействие в расследовании и производстве по гражданско-правовым и административным делам, связанным с противоправными деяниями в сфере использования ИКТ.

4. Ни одно из преступлений, указанных в статьях 6—28 настоящей Конвенции, не рассматривается для целей выдачи и взаимной правовой помощи по уголовным делам, в том числе конфискации и возврата имущества, полученного преступным путем, между государствами-участниками как политическое преступление, преступление, связанное с политическим преступлением, или преступление, совершенное по политическим мотивам. В силу этого запрос о выдаче и оказании правовой помощи по уголовным делам, в том числе по вопросам розыска, ареста, конфискации и возврата имущества, полученного преступным путем, в связи с подобным преступлением не может быть отклонен только на том основании, что он касается политического преступления, или преступления, связанного с политическим преступлением, или преступления, совершенного по политическим мотивам.

При направлении запросов и ответов на них в рамках настоящей Конвенции в экстренных случаях и при достижении договоренности между запрашивающим и запрашиваемым государствами-участниками могут быть использованы каналы Международной организации уголовной полиции — Интерпола.

5. Каждое Государство-участник имеет равное право на защиту информационных ресурсов и критических информационных инфраструктур своего государства от неправомерного использования и несанкционированного вмешательства, в том числе от компьютерных атак на них.

Статья 47. Выдача

1. Настоящая статья применяется к преступлениям, признанным таковыми в соответствии с настоящей Конвенцией, если лицо, выдача которого запрашивается, находится на территории запрашиваемого Государства-участника, при условии, что деяние, в связи с которым запрашивается выдача, является уголовно нака-

зуемым по внутреннему законодательству как запрашивающего Государства-участника, так и запрашиваемого Государства-участника, при условии, что, согласно внутреннему законодательству обоих заинтересованных государств-участников, за совершение этого деяния предусматривается наказание в виде лишения свободы на срок не менее одного года или более суровое наказание.

2. Преступления, предусмотренные статьями 6—28 настоящей Конвенции, считаются включенными в любой существующий между государствами-участниками договор о выдаче в качестве преступлений, которые могут повлечь выдачу. Государства-участники обязуются включать такие преступления в качестве преступлений, которые могут повлечь выдачу, в любой договор о выдаче, который будет заключен между ними. Государство-участник, внутреннее законодательство которого допускает это, в случае, когда оно использует настоящую Конвенцию в качестве основания для выдачи, не считает любое из преступлений, признанных таковыми в соответствии с настоящей Конвенцией, политическим преступлением.

3. Если запрос о выдаче касается нескольких отдельных преступлений, по меньшей мере одно из которых может повлечь за собой выдачу, согласно настоящей статье, а другие не могут повлечь выдачу по причине срока наказания за них, но относятся к преступлениям, признанным таковыми в соответствии с настоящей Конвенцией, запрашиваемое Государство-участник может применить настоящую статью также в отношении этих преступлений.

4. Если Государство-участник, обусловливающее выдачу наличием договора, получает просьбу о выдаче от другого Государства-участника, с которым оно не имеет договора о выдаче, оно может рассматривать настоящую Конвенцию в качестве правового основания для выдачи в связи с любым преступлением, к которому применяется настоящая статья.

5. Государство-участник, обусловливающее выдачу наличием договора:

a) при сдаче на хранение своей ратификационной грамоты или документа о принятии, или утверждении настоящей Конвенции, или присоединении к ней сообщает Генеральному секретарю Организации Объединенных Наций о том, будет ли оно использовать настоящую Конвенцию в качестве правового основания для сотрудничества в вопросах выдачи с другими государствами — участниками настоящей Конвенции; и

b) если оно не использует настоящую Конвенцию в качестве правового основания для сотрудничества в вопросах выдачи, стремится в надлежащих случаях к заключению договоров о выдаче с другими государствами — участниками настоящей Конвенции в целях применения настоящей статьи.

6. Государства-участники, не обусловливающие выдачу наличием договора, в отношениях между собой признают преступления, к которым применяется настоящая статья, в качестве преступлений, которые могут повлечь выдачу.

7. Выдача осуществляется в соответствии с условиями, предусматриваемыми внутренним законодательством запрашиваемого Государства-участника или применимыми договорами о выдаче, включая среди прочего условия, связанные с требованиями о минимальном наказании применительно к выдаче, и основания, на которых запрашиваемое Государство-участник может отказать в выдаче.

8. В отношении любого преступления, к которому применяется настоящая статья, государства-участники при условии соблюдения своего внутреннего законодательства прилагают усилия к тому, чтобы ускорить процедуру выдачи и упростить связанные с ней требования о предоставлении доказательств, если таковые имеются.

9. Запрашиваемое Государство-участник может отказать в выдаче лица, если такая выдача может нанести ущерб его суверенитету, безопасности, общественному порядку или другим существенно важным интересам.

10. При условии соблюдения положений своего внутреннего законодательства и своих договоров о выдаче запрашиваемое Государство-участник, убедившись в том, что обстоятельства требуют этого и носят неотложный характер, и по просьбе запрашивающего Государства-участника, может взять под стражу находящееся на его территории лицо, выдача которого запрашивается, или принять другие надлежащие меры для обеспечения его присутствия в ходе процедуры выдачи, включая передачу выданного лица запрашивающему Государству-участнику.

11. Государство-участник, на территории которого находится лицо, подозреваемое в совершении преступления, если оно не выдает такое лицо в связи с преступлением, к которому применяет-

ся настоящая статья, обязано без каких бы то ни было исключений по просьбе Государства-участника, запрашивающего выдачу, передать дело без неоправданных задержек своим компетентным органам для цели преследования. Эти органы принимают свое решение и осуществляют производство таким же образом, как и в случае любого другого преступления опасного характера, согласно внутреннему законодательству этого Государства-участника. Заинтересованные государства-участники сотрудничают друг с другом, в частности, по процессуальным вопросам и вопросам доказывания, для обеспечения эффективности такого преследования.

12. Во всех случаях, когда Государству-участнику, согласно его внутреннему законодательству, разрешается выдавать или иным образом передавать одного из своих граждан только при условии, что это лицо будет возвращено в это Государство-участник для отбытия наказания, назначенного в результате судебного разбирательства или производства, в связи с которыми запрашивалась выдача или передача этого лица, и это Государство-участник и Государство-участник, запрашивающее выдачу этого лица, согласились с таким порядком и другими условиями, которые они могут счесть надлежащими, такая условная выдача или передача являются достаточными для выполнения обязательства, установленного в пункте 10 настоящей статьи.

13. Любому лицу, по делу которого осуществляется производство в связи с любым преступлением, к которому применяется настоящая статья, гарантируется справедливое обращение на всех стадиях производства, включая осуществление всех прав и гарантий, предусмотренных Международным пактом о гражданских и политических правах и внутренним законодательством Государства-участника, на территории которого находится это лицо.

14. Ничто в настоящей Конвенции не толкуется как устанавливающее обязательство выдачи, если у запрашиваемого Государства-участника имеются существенные основания полагать, что просьба о выдаче имеет целью преследование или наказание какого-либо лица по причине его пола, расы, языка, вероисповедания, гражданства или этнического происхождения или что удовлетворение этой просьбы нанесло бы ущерб положению этого лица по любой из этих причин.

15. До отказа в выдаче запрашиваемое Государство-участник в надлежащих случаях проводит консультации с запрашивающим Государством-участником, с тем чтобы предоставить ему достаточные возможности для изложения его мнений и представления информации, имеющей отношение к изложенным в его запросе фактам.

16. Государства-участники стремятся заключать двусторонние и многосторонние договоры или договоренности с целью осуществления или повышения эффективности выдачи.

17. Каждое Государство-участник назначает центральный орган, ответственный за получение запросов о выдаче и их выполнение. При сдаче на хранение Государством-участником его ратификационной грамоты или документа о принятии или утверждении настоящей Конвенции или присоединении к ней Генеральный секретарь Организации Объединенных Наций уведомляется о центральном органе, назначенном с этой целью.

Статья 48. Non bis in idem

1. Выдача не осуществляется, если компетентные органы запрашиваемого Государства-участника вынесли окончательное решение в отношении запрашиваемого к выдаче лица в связи с преступлением, по поводу которого запрашивается выдача. В выдаче может быть отказано, если компетентные органы запрашиваемого Государства-участника вынесли решение не осуществлять или прекратить судебное преследование в отношении того же преступления.

2. Выдача лица, по делу которого было вынесено окончательное судебное решение в третьем Государстве, являющемся участником Конвенции, в связи с преступлением, в отношении которого запрашивается выдача, не производится:

a) если вышеупомянутое судебное решение освобождает его от ответственности;

b) если срок заключения или другая мера наказания, вынесенная в его отношении:

i) были полностью применены;

ii) стали полностью или в отношении неприменной части предметом помилования или амнистии;

c) если суд осудил преступника без наложения санкций.

3. Вместе с тем в случаях, упоминаемых в пункте 2, решение о выдаче может быть принято:

a) если преступление, в отношении которого было вынесено судебное решение, было совершено против лица, учреждения или

любого субъекта, являющегося публичным должностным лицом запрашивающего Государства;

b) если лицо, в отношении которого было вынесено судебное решение, является публичным должностным лицом запрашивающего Государства;

c) если преступление, в отношении которого было вынесено судебное решение, было совершено полностью или частично на территории запрашивающего Государства или в месте, рассматриваемом как его территория.

4. Положения пунктов 2 и 3 не препятствуют применению более широких внутренних норм, касающихся действия принципа non bis in idem, в отношении судебных решений по уголовным делам, вынесенных в другом Государстве.

Статья 49. Взаимная правовая помощь

1. Государства-участники на взаимной основе оказывают друг другу правовую помощь в целях проведения расследований, преследования или судебного разбирательства в связи с преступлениями и иными противоправными деяниями, совершенными в сфере использования ИКТ.

2. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут быть необходимы для выполнения обязательств, изложенных в статьях 55, 56, 59—62, 66 настоящей Конвенции. Каждое Государство-участник рассматривает также возможность увеличения (продления или приостановления) сроков давности в целях обеспечения неотвратимости ответственности.

3. За исключением случаев, когда положениями статей настоящей главы предусматривается иное, взаимная правовая помощь оказывается на условиях, предусмотренных внутренним законодательством запрашиваемого Государства-участника или положениями применимых договоров о взаимной правовой помощи, включая основания, на которых запрашиваемое Государство-участник может отказаться от сотрудничества полностью или частично.

4. Каждое Государство-участник назначает центральный орган, ответственный за получение запросов о взаимной правовой помощи и их выполнение. При сдаче на хранение Государством-участником его ратификационной грамоты или документа о принятии, или утверждении настоящей Конвенции, или присоединении к ней

Генеральный секретарь Организации Объединенных Наций уведомляется о центральном органе, назначенном с этой целью.

Статья 50. Экстренная взаимная помощь

1. Для целей настоящей статьи чрезвычайная ситуация означает ситуацию, в которой существует значительный и неминуемый риск для жизни или безопасности любого физического лица.

2. Каждое Государство-участник может обратиться к другому Государству-участнику за взаимной помощью в кратчайшие сроки, если оно считает, что существует чрезвычайная ситуация. Запрос в соответствии с настоящей статьей должен включать помимо прочего необходимого содержания описание фактов, свидетельствующих о том, что существует чрезвычайная ситуация, и связь с ней запрашиваемой помощи.

3. Запрашиваемое Государство-участник принимает такой запрос в электронной форме. Однако оно может потребовать обеспечить соответствующий уровень безопасности и аутентификации, прежде чем принимать запрос.

4. Запрашиваемое Государство-участник может в кратчайшие сроки запросить дополнительную информацию для оценки запроса. Запрашивающее Государство-участник предоставляет такую дополнительную информацию в возможно кратчайшие сроки.

5. Убедившись в наличии чрезвычайной ситуации и удовлетворении других требований, необходимых для оказания взаимной помощи, запрашиваемое Государство-участник отвечает на запрос в возможно кратчайшие сроки.

6. Каждое Государство-участник обеспечивает, чтобы должностное лицо его компетентного органа, отвечающее на запросы о взаимной помощи в соответствии со статьями 49 и 52 настоящей Конвенции, было доступно круглосуточно и без выходных для целей реагирования на запрос, направленный в соответствии с данной статьей.

7. Компетентные органы, отвечающие за взаимную помощь, запрашивающего и запрашиваемого государств-участников могут договориться о том, чтобы результаты выполнения запроса в соответствии с настоящей статьей или их предварительная копия могли быть предоставлены запрашивающему Государству-участнику через альтернативный канал связи, отличный от обычно используемого для направления запроса об оказании правовой помощи.

8. В случае возникновения чрезвычайной ситуации запросы могут направляться непосредственно компетентными органами запрашивающего Государства-участника в соответствующие компетентные органы запрашиваемого Государства-участника или через каналы Интерпола или сети 24/7 в соответствии со статьей 66 настоящей Конвенции. В любых таких случаях копия запроса направляется одновременно в центральный орган запрашиваемого Государства-участника через центральный орган запрашивающего Государства-участника. Если запрос направляется непосредственно в центральный орган запрашиваемого Государства-участника и этот орган не является компетентным органом по исполнению запроса, он передает запрос компетентному органу и сообщает центральному органу запрашивающего Государства-участника о передаче такого запроса. Каждое Государство-участник при подписании настоящей Конвенции или при сдаче на хранение ратификационной грамоты или документа о принятии, утверждении или присоединении может сообщить Генеральному секретарю Организации Объединенных Наций, что в целях эффективности запросы, поданные в соответствии с настоящим пунктом, должны направляться только в центральный орган.

Статья 51. Информация, предоставляемая в инициативном порядке

1. Государство-участник может с соблюдением норм своего внутреннего законодательства направить без предварительного запроса другого Государства-участника информацию, полученную в рамках своего расследования, когда, по его мнению, раскрытие такой информации могло бы помочь другому Государству-участнику начать или провести расследование, преследование или судебное разбирательство в отношении преступлений или иных противоправных деяний, признанных таковыми в соответствии с настоящей Конвенцией, или могло бы повлечь за собой направление этим Государством-участником запроса о сотрудничестве в соответствии с положениями настоящей главы.

2. Прежде чем предоставить такую информацию, Государство-участник может просить о соблюдении ее конфиденциальности или определенных условий для ее использования. Если получающее Государство-участник не может выполнить такую просьбу, оно уведомляет об этом предоставляющее Государство-участника, которое определяет затем, следует ли тем не менее предоставить такую информацию. Если получающее Государство-участник принимает информацию на указанных условиях, они носят для нее обязательный характер.

Статья 52. Процедуры направления запросов о взаимной правовой помощи в отсутствие применимых международных договоров

1. В случае, когда между запрашивающим и запрашиваемым государствами-участниками нет действующего договора о взаимной правовой помощи, применяются положения пунктов 2—8 настоящей статьи. При наличии такого договора положения настоящей статьи не применяются, если только заинтересованные государства-участники не соглашаются применять взамен любые или все последующие положения настоящей статьи.

2. a) Каждое Государство-участник назначает центральный орган или органы, которые направляют запросы о взаимной правовой помощи и отвечают на них, организуют исполнение таких запросов или их передачу органам, в компетенцию которых входит их выполнение;

b) центральные органы или иные органы, указанные в подпункте «a», взаимодействуют друг с другом непосредственно;

c) каждое Государство-участник при сдаче на хранение своей ратификационной грамоты или своего документа о принятии, одобрении или присоединении сообщает Генеральному секретарю Организации Объединенных Наций наименования и адреса органов, назначенных в соответствии с настоящим пунктом;

d) Генеральный секретарь Организации Объединенных Наций составляет и постоянно обновляет реестр центральных органов, назначенных государствами-участниками. Каждое Государство-участник обеспечивает, чтобы в этом реестре всегда содержались актуализированные сведения.

3. При исполнении запроса о взаимной правовой помощи органы запрашиваемого Государства-участника применяют законодательство своего государства. По просьбе запрашивающего органа могут применяться процессуальные нормы запрашивающего Государства-участника, если они не противоречат основным принципам правовой системы запрашиваемого Государства-участника.

4. Запрашиваемое Государство-участник может отказать в оказании правовой помощи, если:

a) запрос касается преступления, рассматриваемого запрашиваемым Государством-участником как преступление или как правонарушение, связанное с преступлением против государства;

b) по его мнению, выполнение запроса причинит ущерб его суверенитету, безопасности, публичному порядку или иным существенным интересам.

5. Запрашиваемое Государство-участник может отложить принятие мер по запросу, если такие меры препятствовали бы уголовным расследованиям или судебным разбирательствам, проводимым его компетентными органами.

6. Прежде чем отказать в предоставлении правовой помощи или отсрочить ее оказание, запрашиваемое Государство-участник по мере необходимости после консультаций с запрашивающим Государством-участником рассматривает возможность удовлетворения запроса частично или на таких условиях, какие оно сочтет необходимыми.

7. Запрашиваемое Государство-участник в кратчайшие сроки информирует запрашивающее Государство-участника о результатах выполнения запроса о правовой помощи. В случае отказа в выполнении запроса или отсрочки его выполнения сообщаются причины такого отказа или отсрочки.

8. Запрашивающее Государство-участник может просить запрашиваемое Государство-участника обеспечить конфиденциальность факта и предмета любого запроса, направленного в соответствии с положениями настоящей главы, но лишь в той степени, которая согласуется с его выполнением. Если запрашиваемое Государство-участник не может выполнить просьбу о сохранении конфиденциальности, оно незамедлительно сообщает об этом запрашивающему Государству-участнику, которое затем принимает решение о том, следует ли тем не менее исполнять запрос.

Статья 53. Проведение допроса и иных процессуальных действий с использованием систем видеоконференции или телефонной конференции

1. Компетентные органы Государства-участника по взаимному согласию могут оказывать правовую помощь путем использования систем видеоконференции или телефонной конференции.

2. Использование систем видеоконференции или телефонной конференции осуществляется в соответствии с законодательством запрашиваемого Государства-участника. Если запрашиваемое Государство-участник не имеет доступа к техническим средствам для проведения видеоконференции, такие средства по взаимной договоренности могут быть предоставлены ему запрашивающим Государством-участником.

Статья 54. Полномочия дипломатических представительств и консульских учреждений

1. Государства-участники имеют право вручать документы собственным гражданам через свои дипломатические представительства или консульские учреждения.

2. Государства-участники имеют право по поручению своих компетентных органов допрашивать собственных граждан через свои дипломатические представительства или консульские учреждения, в том числе с использованием систем видеоконференцсвязи или телефонной конференции.

3. В случаях, указанных в пунктах 1 и 2 настоящей статьи, нельзя применять средства принуждения или угрозу ими.

Статья 55. Конфиденциальность и ограничения на использование информации

1. В случае отсутствия между запрашивающим и запрашиваемым государствами-участниками действующего договора о взаимной правовой помощи, опирающегося на единообразное или основанное на принципе взаимности законодательство, применяются положения настоящей статьи. Положения настоящей статьи при наличии такого договора или законодательства не применяются, если только заинтересованные государства-участники не соглашаются применять вместо последних любые или все последующие положения настоящей статьи.

2. В ответ на просьбу запрашиваемое Государство-участник может выдвинуть следующие условия предоставления информации или материала:

a) сохранение их конфиденциальности, если без такого условия просьба о взаимной правовой помощи не могла бы быть выполнена;

b) неиспользование для других расследований или судебных разбирательств, которые не указываются в просьбе.

3. Если запрашивающее Государство-участник не может выполнить одно из условий, упомянутых в пункте 2 настоящей статьи, оно незамедлительно информирует об этом другое Государство-участника, которое затем решает, может ли быть предоставлена такая информация. Если запрашивающее Государство-участник соглашается выполнить эти условия, они приобретают для него обязательную силу.

4. Любое Государство-участник, предоставляющее информацию или материал на упомянутых в пункте 2 настоящей статьи условиях, может в связи с одним из условий потребовать от другого Государства-участника разъяснения относительно имевшего место использования такой информации или материала.

Статья 56. Защита персональных данных

1. Персональные данные, передаваемые одним Государством-участником другому Государству-участнику на основании запроса, сделанного в соответствии с настоящей Конвенцией, могут быть использованы Государством-участником, которому переданы эти данные, только для целей производства по уголовному, административному или гражданскому делу, других судебных или административных процедур, напрямую связанных с этим производством, а также для предотвращения непосредственной и серьезной угрозы общественной безопасности и лиц, чьи персональные данные передаются.

2. Такие персональные данные не могут быть переданы третьей стороне без предварительного письменного согласия Государства-участника, из которого были переданы данные, или субъекта персональных данных.

3. Государство-участник, которое передает персональные данные на основании запроса, сделанного в соответствии с настоящей Конвенцией, может потребовать от Государства-участника, которому переданы данные, предоставление информации об их использовании.

Статья 57. Передача уголовного производства

Государства-участники рассматривают возможность взаимной передачи производства в целях уголовного преследования в связи с преступлением, охватываемым настоящей Конвенцией, в случаях, когда считается, что такая передача отвечает интересам надлежащего отправления правосудия, в частности, в случаях, когда затрагиваются несколько юрисдикций, для обеспечения объединения уголовных дел.

Статья 58. Передача осужденных лиц

Государства-участники рассматривают возможность заключения двусторонних или многосторонних договоров или иных договоренностей о передаче лиц, осужденных к тюремному заключению или другим видам лишения свободы за преступления, признанные таковыми в соответствии с настоящей Конвенцией, с тем чтобы такие лица могли отбывать срок наказания на территории этих государств-участников.

Статья 59. Оперативное обеспечение сохранности информации в электронной форме

1. Любое Государство-участник может просить другое Государство-участника дать указание или принять иные меры с целью безотлагательно обеспечить сохранность информации, которая хранится или обрабатывается с использованием ИКТ на территории этого Государства-участника и в отношении которой запрашивающее Государство-участник намеревается в рамках взаимной правовой помощи направить запрос об обыске, выемке или об ином обеспечении сохранности или получении этой информации.

2. В запросе об обеспечении сохранности информации, направляемом в соответствии с пунктом 1 настоящей статьи, указываются:

a) наименование запрашивающего органа;

b) краткое изложение основных фактов, характер расследования, преследования или судебного разбирательства, к которым относится запрос;

c) информация в электронной форме, подлежащая сохранению, и ее связь с преступлением или правонарушением, в связи с которым направлен запрос;

d) любые имеющиеся сведения, идентифицирующие владельца информации или местоположение устройства ИКТ;

e) обоснование необходимости обеспечения сохранности информации;

f) сообщение о том, что это Государство-участник намеревается в рамках взаимной правовой помощи направить запрос об обыске, выемке или об ином обеспечении сохранности этой информации.

3. По получении такого запроса от другого Государства-участника запрашиваемое Государство-участник в соответствии со своим внутренним законодательством принимает надлежащие меры для оперативного обеспечения сохранности информации, указанной в пункте 1 настоящей статьи. Запрашиваемое Государство-участник может исполнить частично либо полностью запрос об обеспечении сохранности информации, даже если деяние, послужившее основанием для запроса, не является уголовно наказуемым в запрашиваемом Государстве-участнике.

4. В исполнении запроса об обеспечении сохранности информации может быть отказано, если запрашиваемое Государство-участник полагает, что исполнение такого запроса может нанести ущерб его суверенитету, безопасности или другим существенным интересам.

5. Если запрашиваемое Государство-участник полагает, что исполнение запроса, указанного в пункте 1 настоящей статьи, не обеспечит в дальнейшем сохранности информации, или поставит под угрозу обеспечение конфиденциальности, или иным образом помешает проводимому расследованию, преследованию или судебному разбирательству, оно незамедлительно уведомляет об этом запрашивающее Государство-участника. На основании такого уведомления запрашивающее Государство-участник принимает решение о необходимости исполнения запроса.

6. Любое обеспечение сохранности информации, предпринятое в рамках исполнения запроса, указанного в пункте 1 настоящей статьи, производится на срок не менее 90 дней для того, чтобы запрашивающее Государство-участник могло направить запрос об обыске, выемке или об ином обеспечении сохранности этой информации. После получения такого запроса запрашиваемое Государство-участник сохраняет эту информацию до принятия решения по запросу.

Статья 60. Оперативное предоставление сохраненных технических параметров трафика

1. Если в ходе исполнения запроса об обеспечении сохранности информации в соответствии со статьей 59 настоящей Конвенции запрашиваемому Государству-участнику станет известно, что в передаче информации участвовал поставщик услуг с территории иного государства, оно оперативно раскрывает в порядке, установленном национальным законодательством, запрашивающему Государству-

участнику технические параметры трафика в объеме, позволяющем идентифицировать этого поставщика услуг и определить маршрут передачи информации, сохранение которой запрашивается.

2. В исполнении запроса об обеспечении сохранности информации может быть отказано, если запрашиваемое Государство-участник полагает, что исполнение такого запроса может нанести ущерб его суверенитету, безопасности или другим существенным интересам.

Статья 61. Взаимная помощь по сбору технических параметров трафика в режиме реального времени

1. Государство-участник по запросу другого Государства-участника осуществляет на своей территории или территории, находящейся под его юрисдикцией, сбор технических параметров трафика в режиме реального времени и затем, в соответствии с процедурами, предусмотренными внутренним законодательством, при наличии соответствующих оснований передает собранную информацию запрашивающему Государству-участнику.

2. В запросе, направляемом в соответствии с пунктом 1 настоящей статьи, указываются:

a) наименование запрашивающего органа;

b) краткое изложение основных фактов, характер расследования, преследования или судебного разбирательства, к которым относится запрос;

c) информация в электронной форме, относительно которой требуется сбор технических параметров трафика, и ее связь с преступлением или иным противоправным деянием;

d) любые имеющиеся сведения, идентифицирующие владельца/пользователя информации или местоположение устройства ИКТ;

e) обоснование необходимости сбора технических параметров трафика, обоснование указанного периода сбора технических параметров трафика;

f) период сбора технических параметров трафика.

Статья 62. Взаимная помощь по сбору информации в электронной форме

Государство-участник осуществляет на своей территории или территории, находящейся под его юрисдикцией, сбор информации

в электронно-цифровой форме, включающей данные о содержании сообщений, в режиме реального времени, передаваемой с использованием ИКТ, в соответствии с процедурами, предусмотренными его внутренним законодательством. Предоставление другому Государству-участнику такой информации осуществляется в соответствии с внутренним законодательством Государства-участника, осуществляющего сбор информации, а также действующими договорами о взаимной правовой помощи.

Статья 63. Совместные расследования

По взаимному соглашению компетентные органы двух или более государств-участников могут создавать совместные следственные группы для определенной цели и на ограниченный период, который может быть продлен по взаимному согласию, для проведения уголовных расследований в одном или нескольких государствах-участниках, создавших группу. С этой целью государства-участники рассматривают возможность заключения двусторонних или многосторонних соглашений или договоренностей. Состав группы определяется в соглашении.

Просьба о создании совместной следственной группы может исходить от любого заинтересованного Государства-участника. Группа создается в одном из государств-участников, в котором предполагается проведение расследования.

Государства-участники обеспечивают полное уважение суверенитета Государства-участника, на территории которого должно быть проведено такое расследование.

Статья 64. Специальные методы расследования

1. В целях эффективной борьбы с преступлениями в сфере использования ИКТ каждое Государство-участник в той мере, в какой это допускается основными принципами его внутреннего права, и на условиях, установленных законодательством, принимает в пределах своих возможностей необходимые меры, какие могут потребоваться, с тем чтобы разрешить надлежащее применение его компетентными органами контролируемых поставок и других специальных методов расследования, таких как электронное наблюдение или другие формы наблюдения, а также агентурные операции его компетентными органами на его территории, и чтобы доказательства, собранные с помощью таких методов, допускались в суде.

2. Для цели расследования преступлений, охватываемых настоящей Конвенцией, государства-участники поощряются к заключению при необходимости соответствующих двусторонних или многосторонних соглашений или договоренностей для использования таких специальных методов расследования в контексте сотрудничества на международном уровне. Такие соглашения или договоренности заключаются и осуществляются при полном соблюдении принципа суверенного равенства государств и реализуются в строгом соответствии с условиями этих соглашений или договоренностей.

3. В отсутствие соглашения или договоренности, указанных в пункте 2 настоящей статьи, решения об использовании таких специальных методов расследования на международном уровне принимаются в каждом отдельном случае и могут при необходимости учитывать финансовые договоренности и взаимопонимание в отношении осуществления юрисдикции заинтересованными государствами-участниками.

Статья 65. Сотрудничество между правоохранительными органами

1. Государства-участники тесно сотрудничают друг с другом, действуя сообразно своим внутренним правовым и административным системам, в целях повышения эффективности правоприменительных мер для борьбы с преступлениями, охватываемыми настоящей Конвенцией. Государства-участники, в частности, принимают эффективные меры, направленные:

a) на укрепление или, где это необходимо, установление каналов связи между их компетентными органами, учреждениями и службами, с тем чтобы обеспечить надежный и быстрый обмен информацией о всех аспектах преступлений, охватываемых настоящей Конвенцией, включая, если заинтересованные государства-участники сочтут это надлежащим, связи с другими видами преступной деятельности;

b) сотрудничество с другими государствами-участниками в проведении расследований в связи с преступлениями, охватываемыми настоящей Конвенцией, в целях выявления:

i) личности, местонахождения и деятельности лиц, подозреваемых в участии в совершении таких преступлений, или местонахождения других причастных лиц;

ii) перемещения доходов от преступлений или имущества, полученного в результате совершения таких преступлений;

iii) перемещения имущества, орудий, оборудования или других средств, использовавшихся или предназначавшихся для использования при совершении таких преступлений;

c) передачу предметов, которые были использованы при совершении преступлений, в том числе орудий преступлений; предметов, которые были приобретены в результате преступлений или в качестве вознаграждения за них, или же предметов, которые преступник получил взамен приобретенных таким образом; и предметов, которые могут иметь значение доказательств в уголовном деле;

d) обмен в надлежащих случаях с другими государствами-участниками информацией о конкретных средствах и методах, применяемых для совершения преступлений, охватываемых настоящей Конвенцией, включая образцы вредоносного программного обеспечения, использование поддельных удостоверений личности, фальшивых, измененных или поддельных документов и других средств для сокрытия противоправной деятельности;

e) содействие эффективной координации между их компетентными органами, учреждениями и службами и поощрение обмена сотрудниками и другими экспертами, включая, при условии заключения заинтересованными государствами-участниками двусторонних соглашений или договоренностей, направление сотрудников по связям;

f) обмен представляющей интерес информацией и проведение скоординированных мероприятий с целью заблаговременного выявления преступлений, охватываемых настоящей Конвенцией.

2. Для целей практического применения настоящей Конвенции государства-участники рассматривают возможность заключения двусторонних или многосторонних соглашений или договоренностей о непосредственном сотрудничестве между их правоохранительными органами, а в тех случаях, когда такие соглашения или договоренности уже имеются, их совершенствования. В отсутствие таких соглашений или договоренностей между заинтересованными государствами-участниками государства-участники могут рассматривать настоящую Конвенцию в качестве основы для взаимного сотрудничества между правоохранительными

органами в отношении преступлений, охватываемых настоящей Конвенцией. В надлежащих случаях государства-участники в полной мере используют соглашения или договоренности, в том числе механизмы международных или региональных организаций, для расширения сотрудничества между своими правоохранительными органами.

Каждое Государство-участник может в экстренных ситуациях направлять запросы об оказании содействия или сообщения, связанные с такими запросами, используя оперативные средства связи, включая факсимильную связь или электронную почту, в той мере, в какой такие средства обеспечивают соответствующие уровни безопасности и подтверждение подлинности (включая, если необходимо, использование шифрования), с последующим официальным подтверждением, если того требует запрашиваемое Государство-участник. Запрашиваемое Государство-участник принимает такой запрос и отвечает на него с помощью любых аналогичных оперативных средств связи. Запрашиваемое Государство-участник может оставить за собой право направить ответ после получения оригинала запроса, о чем уведомляет депозитария.

Статья 66. Сеть 24/7

1. Каждое Государство-участник назначает контактный центр, работающий 24 часа в сутки 7 дней в неделю и призванный обеспечивать оперативное содействие в проведении расследований, преследований или судебных разбирательств в связи с преступлениями, имеющими отношение к компьютерным системам и данным, или в сборе доказательств в электронно-цифровой форме в отношении преступлений. Такая помощь включает поддержку применения или, если это допускается внутренним правом или практикой, непосредственное применение следующих мер:

a) оказание технической консультативной помощи;

b) обеспечение сохранности данных в целях сбора доказательств и последующего предоставления информации в соответствии с его внутренним законодательством, а также действующими договорами о взаимной правовой помощи.

2. Каждое Государство-участник принимает меры для предоставления квалифицированного персонала и оборудования с целью облегчить функционирование такой сети.

Раздел 2
Меры по возвращению имущества

Статья 67. Общие положения

Государства-участники самым широким образом сотрудничают друг с другом и предоставляют друг другу взаимную правовую помощь по возвращению имущества, полученного преступным путем, в соответствии с положениями настоящей Конвенции и внутренним законодательством и с учетом соответствующих инициатив международных региональных и межрегиональных организаций по противодействию отмыванию денежных средств.

Статья 68. Предупреждение и выявление переводов доходов от преступлений

1. Государство-участник принимает все необходимые меры, позволяющие в соответствии с внутренним законодательством получать от финансовых учреждений, а также организаций, осуществляющих деятельность, связанную с оборотом цифровых финансовых активов и цифровой валюты, на которые распространяется его юрисдикция, информацию о личности клиентов и собственников-бенефициаров, в отношении которых имеется информация об их возможной причастности или о возможной причастности членов их семей или тесно связанных с ними партнеров или лиц, действующих от их имени, к совершению преступлений, предусмотренных положениями настоящей Конвенции, включая информацию о счетах всех вышеперечисленных лиц.

2. Государство-участник принимает все необходимые меры, позволяющие в соответствии с внутренним законодательством требовать от финансовых учреждений, а также организаций, осуществляющих деятельность, связанную с оборотом цифровых финансовых активов и цифровой валюты, принятия разумных мер контроля в отношении счетов, которые пытаются открыть или которые ведут лица, указанные в пункте 1 настоящей статьи.

3. Меры, указанные в пунктах 1 и 2 настоящей статьи, в разумной степени призваны выявлять подозрительные операции для целей представления информации о них компетентным органам и не должны толковаться как препятствующие или запрещающие финансовым учреждениям, а также организациям, осуществляющим

деятельность, связанную с оборотом цифровых финансовых активов и цифровой валюты, вести дела с любым законным клиентом.

4. С целью содействия осуществлению мер, предусмотренных в пунктах 1 и 2 настоящей статьи, каждое Государство-участник в надлежащих случаях уведомляет финансовые учреждения, а также организации, осуществляющие деятельность, связанную с оборотом цифровых финансовых активов и цифровой валюты, на которые распространяется его юрисдикция, по просьбе другого Государства-участника или по своей собственной инициативе, о личностях конкретных физических или юридических лиц, в отношении счетов которых от таких учреждений и организаций будет ожидаться применение более жестких мер контроля, в дополнение к тем лицам, личности которых финансовые учреждения, а также организации, осуществляющие деятельность, связанную с оборотом цифровых финансовых активов и цифровой валюты, могут установить в ином порядке.

5. Каждое Государство-участник осуществляет меры для обеспечения того, чтобы его финансовые учреждения, а также организации, осуществляющие деятельность, связанную с оборотом цифровых финансовых активов и цифровой валюты, сохраняли в течение надлежащего срока должную отчетность о счетах и операциях, к которым причастны лица, упомянутые в пункте 1 настоящей статьи, в которую должна включаться как минимум информация, касающаяся личности клиента, а также, насколько это возможно, собственника-бенефициара.

6. С целью предупреждения и выявления переводов доходов от преступлений, признанных таковыми в соответствии с настоящей Конвенцией, каждое Государство-участник осуществляет надлежащие и действенные меры для предупреждения, при помощи своих регулирующих и надзорных органов, учреждения банков, которые не имеют физического присутствия и которые не аффилированы с какой-либо регулируемой финансовой группой. Кроме того, государства-участники рассматривают возможность установления по отношению к своим финансовым учреждениям, а также организациям, осуществляющим деятельность, связанную с оборотом цифровых финансовых активов и цифровой валюты, требования отказываться вступать в корреспондентские банковские отношения с такими учреждениями или продолжать такие отношения, а также

остерегаться устанавливать отношения с иностранными финансовыми учреждениями, разрешающими использование счетов в них банками, которые не имеют физического присутствия или которые не аффилированы с какой-либо регулируемой финансовой группой.

7. Каждое Государство-участник рассматривает возможность создания в соответствии со своим внутренним законодательством эффективных систем, предусматривающих раскрытие финансовой информации относительно лиц, в отношении которых имеется информация о возможной причастности к совершению преступлений, предусмотренных положениями настоящей Конвенции, и устанавливает надлежащие санкции за несоблюдение требований, указанных в настоящей статье. Каждое Государство-участник рассматривает также возможность принятия таких мер, какие могут потребоваться, с тем чтобы позволить своим компетентным органам осуществлять обмен такой информацией с компетентными органами в других государствах-участниках, когда это необходимо для расследования и принятия мер по возвращению доходов от преступлений, признанных таковыми в соответствии с настоящей Конвенцией.

Статья 69. Меры для непосредственного возвращения имущества

Каждое Государство-участник в соответствии со своим внутренним законодательством принимает такие законодательные или иные меры, которые могут потребоваться, с тем чтобы:

a) разрешить другому Государству-участнику, его гражданам и лицам без гражданства, постоянно проживающим на его территории, и юридическим лицам, учрежденным или имеющим постоянное представительство на его территории, предъявлять в суды этого Государства-участника гражданские иски об установлении имущественного права, нарушенного в результате совершения какого-либо из преступлений или иных противоправных деяний, признанных таковыми в соответствии с настоящей Конвенцией;

b) позволить своим судам выносить решения о выплате компенсации или возмещении ущерба, нанесенного в результате совершения таких преступлений и иных противоправных деяний, признанных таковыми в соответствии с настоящей Конвенцией; и

c) позволить своим судам или компетентным органам при вынесении решений о конфискации признавать полностью или частично требования другого Государства-участника, его граждан и лиц

без гражданства, постоянно проживающих на его территории, и юридических лиц, учрежденных или имеющих постоянное представительство на его территории, как законного собственника имущества, приобретенного в результате совершения какого-либо из преступлений или иных противоправных деяний, признанных таковыми в соответствии с настоящей Конвенцией.

Статья 70. Механизмы изъятия имущества посредством международного сотрудничества в деле конфискации

1. Каждое Государство-участник в целях предоставления взаимной правовой помощи в отношении имущества, приобретенного в результате совершения какого-либо из преступлений, признанных таковыми в соответствии с настоящей Конвенцией, или средств совершения таких преступлений, в соответствии со своим внутренним законодательством:

a) принимает такие меры, какие могут потребоваться, с тем чтобы позволить своим компетентным органам приводить в исполнение постановления о конфискации, вынесенные судами другого Государства-участника;

b) в пределах своей юрисдикции принимает такие меры, какие могут потребоваться, с тем чтобы позволить своим компетентным органам конфисковать имущество иностранного происхождения по судебному решению в связи с легализацией доходов, полученных в результате совершения преступления, признанного таковым в соответствии с положениями настоящей Конвенции;

c) рассматривает вопрос о принятии таких мер, какие могут потребоваться, с тем чтобы создать возможность для конфискации такого имущества без вынесения приговора в рамках уголовного производства по делам, когда преступник не может быть подвергнут преследованию по причине смерти, укрывательства или отсутствия или в других соответствующих случаях.

2. Каждое Государство-участник в целях предоставления взаимной правовой помощи по просьбе другого Государства-участника в соответствии со своим внутренним законодательством:

a) принимает такие меры, какие могут потребоваться, с тем чтобы позволить своим компетентным органам налагать арест на имущество согласно постановлению об аресте, которое вынесено судом или другим компетентным органом запрашивающего Госу-

дарства-участника и в котором излагаются разумные основания, позволяющие запрашиваемому Государству-участнику полагать, что существуют достаточные мотивы для принятия таких мер и что в отношении этого имущества будет в итоге вынесено постановление о конфискации для целей пункта 1(a) настоящей статьи;

b) принимает такие меры, какие могут потребоваться, с тем чтобы позволить своим компетентным органам налагать арест на имущество по запросу, в котором излагаются разумные основания, позволяющие запрашиваемому Государству-участнику полагать, что существуют достаточные мотивы для принятия таких мер и что в отношении этого имущества будет в итоге вынесено постановление о конфискации для целей пункта 1(a) настоящей статьи;

c) рассматривает вопрос о принятии дополнительных мер, с тем чтобы позволить своим компетентным органам сохранять имущество для целей конфискации, например, на основании иностранного постановления об аресте или предъявления уголовного обвинения в связи с приобретением подобного имущества.

3. Предоставление правовой помощи в соответствии с пунктом 2 настоящей статьи осуществляется на основании соответствующего запроса, направляемого в письменной форме.

4. При возникновении сомнения в подлинности или содержании запроса может быть запрошено его дополнительное подтверждение.

5. Запрос должен содержать:

a) наименование компетентного органа, запрашивающего содействие, и запрашиваемого компетентного органа;

b) изложение существа дела;

c) указание цели и обоснование запроса;

d) описание содержания запрашиваемого содействия;

e) копию постановления об аресте, если имеется;

f) любую другую информацию, которая может быть полезна для надлежащего исполнения запроса.

6. Запрос, переданный или подтвержденный в письменной форме, подписывается уполномоченным должностным лицом запрашивающего компетентного органа и удостоверяется печатью этого органа.

Статья 71. Международное сотрудничество в целях конфискации

1. Государство-участник, получившее от другого Государства-участника, под юрисдикцию которого подпадает какое-либо преступление, признанное таковым в соответствии с настоящей Конвенцией, запрос о конфискации упомянутого в пункте 1 статьи настоящей Конвенции имущества, полученного в результате совершения преступлений, предусмотренных настоящей Конвенцией, или средств совершения таких преступлений, находящихся на его территории, в той степени, в которой это разрешено его внутренним законодательством:

a) направляет этот запрос своим компетентным органам с целью получения решения о конфискации и в случае вынесения такого решения приводит его в исполнение; или

b) направляет своим компетентным органам решение о конфискации, вынесенное судом на территории запрашивающего Государства-участника, с целью его исполнения в том объеме, который указан в просьбе, и в той мере, в какой оно относится к находящемуся на территории запрашиваемого Государства-участника имуществу, полученному в результате совершения преступлений, признанных таковыми в соответствии с настоящей Конвенцией, или к средствам совершения таких преступлений.

2. По получении запроса, направленного другим Государством-участником, под юрисдикцию которого подпадает какое-либо преступление, признанное таковым в соответствии с настоящей Конвенцией, запрашиваемое Государство-участник принимает меры для выявления или ареста имущества, полученного в результате совершения преступлений, признанных таковыми в соответствии с настоящей Конвенцией, или средств совершения таких преступлений, упомянутых в пункте 1(b) настоящей статьи, с целью последующей конфискации, решение о которой выносится либо запрашивающим Государством-участником, либо запрашиваемым Государством-участником в соответствии с запросом согласно пункту 1 настоящей статьи.

3. Решения или меры, предусмотренные в пунктах 1 и 2 настоящей статьи, принимаются запрашиваемым Государством-участником в соответствии с положениями его внутреннего законодательства и любыми двусторонними или многосторонними соглашениями или договоренностями, которыми оно может быть связано в отношениях с запрашивающим Государством-участником.

4. Каждое Государство-участник представляет Генеральному секретарю Организации Объединенных Наций тексты своих зако-

нов и правил, обеспечивающих осуществление положений настоящей статьи, а также тексты любых последующих изменений к таким законам и правилам или их описание.

5. В исполнении запроса, направленного в соответствии с настоящей статьей, может быть отказано или же обеспечительные меры могут быть сняты, если запрашиваемое Государство-участник своевременно не получит постановление компетентного органа запрашивающего Государства-участника или документы, необходимые для принятия компетентным органом запрашиваемого Государства-участника такого решения.

6. До снятия любой обеспечительной меры, принятой в соответствии с настоящей статьей, запрашиваемое Государство-участник, когда это возможно, предоставляет запрашивающему Государству-участнику возможность представить обоснование (изложить свои мотивы в пользу) продолжения осуществления такой меры.

7. Положения настоящей статьи не толкуются таким образом, чтобы наносился ущерб правам добросовестных третьих сторон.

Статья 72. Специальное сотрудничество

Без ущерба для своего внутреннего законодательства каждое Государство-участник стремится принимать меры, позволяющие ему в инициативном порядке и если это не наносит ущерб проводимым его компетентными органами уголовным расследованиям или судебным разбирательствам, направлять информацию об имуществе, полученном в результате совершения преступлений, признанных таковыми в соответствии с настоящей Конвенцией, другому Государству-участнику, когда оно считает, что раскрытие такой информации может послужить основанием для проведения уголовного расследования или судебного разбирательства компетентными органами получающего Государства-участника или может привести к направлению этим Государством-участником запроса в соответствии с настоящей главой.

Статья 73. Возвращение похищенного имущества и распоряжение им

1. Государство-участник, конфисковавшее имущество в соответствии с положениями настоящей главы, распоряжается им, включая возвращение такого имущества его предыдущим законным собственникам, согласно пункту 3 настоящей статьи и своему внутреннему законодательству.

2. Каждое Государство-участник принимает такие законодательные и иные меры, которые могут потребоваться для того, чтобы позволить своим компетентным органам возвращать конфискованное имущество, когда они действуют по запросу, направленному другим Государством-участником в соответствии с настоящей Конвенцией, с учетом прав добросовестных третьих сторон и в соответствии со своим внутренним законодательством.

3. В соответствии со статьей 71 настоящей Конвенции и пунктами 1 и 2 настоящей статьи запрашиваемое Государство-участник:

a) в случае хищения публичного имущества, если конфискация была произведена в соответствии со статьей 68 настоящей Конвенции и на основании окончательного судебного решения, вынесенного в запрашивающем Государстве-участнике, причем это требование может быть снято запрашиваемым Государством-участником, возвращает конфискованное имущество запрашивающему Государству-участнику;

b) во всех других случаях в первоочередном порядке рассматривает вопрос о возвращении конфискованного имущества его предыдущим законным собственникам, или выплате компенсации, или возмещении ущерба потерпевшим от преступления.

4. В надлежащих случаях, если только государства-участники не примут иного решения, запрашиваемое Государство-участник может вычесть разумные расходы, понесенные в ходе расследования или судебного разбирательства, которые привели к возвращению конфискованного имущества или распоряжению им, согласно настоящей статье.

5. В целях достижения взаимоприемлемых договоренностей относительно окончательного распоряжения конфискованным имуществом государства-участники могут проводить консультации и заключать отдельные соглашения.

Статья 74. Расходы

Обычные расходы, связанные с выполнением запроса, покрываются запрашиваемым Государством-участником, если заинтересованные государства-участники не договорились об ином. Если выполнение запроса требует существенных или чрезвычайных расходов, то государства-участники проводят консультации с целью определения условий, на которых будет выполнен запрос, а также порядка покрытия расходов.

Глава V
Техническая помощь и подготовка кадров

Статья 75. Общие принципы технической помощи

1. Государства-участники с учетом своих возможностей рассматривают вопрос о предоставлении друг другу широкой технической помощи, особенно в интересах развивающихся стран, в связи с их соответствующими планами и программами по борьбе с преступлениями в сфере ИКТ, включая подготовку кадров в областях, указанных в статье 76 настоящей Конвенции, а также подготовку кадров и оказание помощи и взаимный обмен соответствующим опытом и специальными знаниями, что будет способствовать международному сотрудничеству между государствами-участниками по вопросам выдачи, взаимной правовой помощи.

2. Государства-участники активизируют, насколько это необходимо и возможно, усилия, направленные на максимальное повышение эффективности практических и учебных мероприятий в международных и региональных организациях и в рамках соответствующих двусторонних и многосторонних соглашений или договоренностей.

3. Государства-участники рассматривают возможность оказания друг другу содействия в проведении оценок, исследований и разработок, касающихся видов, причин и последствий преступлений, совершаемых в сфере ИКТ в государствах-участниках, с целью разработки с участием компетентных органов, общества и частного сектора стратегий и планов действий по борьбе с этими видами преступлений.

4. Государства-участники поручают Управлению Организации Объединенных Наций по наркотикам и преступности оказывать государствам-участникам профильную техническую помощь в целях содействия реализации программ и проектов по борьбе с преступлениями и иными правонарушениями в сфере ИКТ.

Статья 76. Подготовка кадров

1. Каждое Государство-участник, насколько это необходимо, разрабатывает, осуществляет или совершенствует конкретные программы подготовки персонала, несущего ответственность за предупреждение преступлений в сфере ИКТ и борьбу с ними. Такие программы подготовки кадров могут затрагивать среди прочего следующие области:

a) эффективные меры по предупреждению, выявлению и расследованию преступлений в сфере ИКТ, а также наказанию за их совершение и борьбе с ними, включая методы сбора и использования доказательств в электронной форме и расследования;

b) наращивание потенциала в области разработки и планирования стратегической политики противодействия преступлениям в сфере ИКТ;

c) подготовка сотрудников компетентных органов по вопросам составления запросов о выдаче, взаимной правовой помощи и правоохранительном содействии, удовлетворяющих требованиям настоящей Конвенции;

d) предупреждение перевода доходов от преступлений, признанных таковыми в соответствии с настоящей Конвенцией, а также изъятие таких доходов;

e) выявление и приостановление операций по переводу доходов от преступлений, признанных таковыми в соответствии с настоящей Конвенцией;

f) отслеживание перемещения доходов от преступлений, признанных таковыми в соответствии с настоящей Конвенцией, и методов, используемых для перевода, сокрытия или утаивания таких доходов;

g) надлежащие и действенные правовые и административные механизмы и методы, способствующие изъятию и конфискации доходов от преступлений, признанных таковыми в соответствии с настоящей Конвенцией;

h) методы, используемые в защите потерпевших и свидетелей, которые сотрудничают с судебными и правоохранительными органами; и

i) подготовка сотрудников по вопросам, касающимся внутригосударственных и международных правил, и языковая подготовка.

2. Государства-участники при содействии Управления Организации Объединенных Наций по наркотикам и преступности и других международных организаций могут оказывать государствам-участникам профильную помощь в подготовке кадров в целях содействия реализации национальных программ и проектов по борьбе с преступлениями в сфере ИКТ.

Статья 77. Обмен информацией

1. Каждое Государство-участник рассматривает возможность проведения в консультации с экспертами анализа тенденций пре-

ступности в сфере ИКТ на своей территории и обстоятельств совершения таких преступлений.

2. Государства-участники в целях разработки, насколько это возможно, общих определений, стандартов и методологий рассматривают возможность распространения статистических данных и аналитических знаний о преступлениях в сфере ИКТ, в том числе об оптимальных видах практики в деле предупреждения таких преступлений и борьбы с ними, и обмениваются этими данными между собой и через посредство международных и региональных организаций.

3. Каждое Государство-участник рассматривает возможность осуществления надлежащего контроля за своей политикой и практическими мерами по борьбе с преступлениями в сфере ИКТ, а также проведения оценки их эффективности.

Глава VI
Механизмы выполнения Конвенции

Статья 78. Конференция государств — участников Конвенции

1. Настоящим учреждается Конференция государств — участников Конвенции в целях расширения возможностей государств-участников и сотрудничества между ними для достижения целей, установленных в настоящей Конвенции, а также содействия выполнению настоящей Конвенции и проведения обзора ее осуществления.

2. Генеральный секретарь Организации Объединенных Наций созывает Конференцию государств-участников не позднее чем через один год после вступления в силу настоящей Конвенции. Впоследствии в соответствии с правилами процедуры, принятыми Конференцией государств-участников, проводятся очередные сессии Конференции.

3. Конференция государств-участников принимает правила процедуры и правила, регулирующие осуществление видов деятельности, указанных в настоящей статье, в том числе правила, касающиеся допуска и участия наблюдателей и оплаты расходов, понесенных при осуществлении этих видов деятельности.

4. Конференция государств-участников согласовывает виды деятельности, процедуры и методы работы для достижения целей, изложенных в пункте 1 настоящей статьи, включая:

a) содействие деятельности государств-участников согласно статьям 76—77 и главам II—VI настоящей Конвенции, в том числе путем поощрения мобилизации добровольных взносов;

b) содействие обмену между государствами-участниками информацией о формах преступлений в сфере ИКТ и тенденциях в этой области, а также об успешных методах предупреждения указанных преступлений, борьбы с ними, за исключением сведений, составляющих государственную тайну в соответствии с законодательством Государства-участника, и возвращения доходов от преступлений;

c) сотрудничество с соответствующими международными и региональными организациями и механизмами и международными неправительственными организациями;

d) надлежащее использование соответствующей информации, подготовленной другими международными и региональными механизмами в целях предупреждения преступлений в сфере ИКТ и борьбы с ними, во избежание излишнего дублирования работы;

e) периодическое рассмотрение вопроса об осуществлении настоящей Конвенции ее государствами-участниками; вынесение рекомендаций, касающихся совершенствования настоящей Конвенции и ее выполнения;

f) учет потребностей государств-участников в технической помощи в связи с выполнением настоящей Конвенции и вынесение рекомендаций в отношении любых действий, которые она может считать необходимыми в связи с этим.

5. Для цели пункта 4 настоящей статьи Конференция государств-участников получает необходимые сведения о мерах, принятых государствами-участниками в ходе выполнения настоящей Конвенции, и трудностях, с которыми они при этом столкнулись, на основе предоставленной ими информации и через посредство таких дополнительных механизмов проведения обзора, какие могут быть созданы Конференцией государств-участников.

6. Каждое Государство-участник представляет Конференции государств-участников информацию о законодательных и административных и иных мерах, а также о своих программах, планах и практике, направленных на выполнение настоящей Конвенции, как это требуется Конференции государств-участников. Конференция государств-участников изучает вопрос о наиболее эффективных

путях получения такой информации и принятия на ее основе соответствующих решений, включая среди прочего информацию, полученную от государств-участников и от компетентных международных организаций. Могут быть рассмотрены также материалы, полученные от соответствующих международных неправительственных организаций, надлежащим образом аккредитованных в соответствии с процедурами, которые будут определены решением Конференции государств-участников.

7. Согласно пунктам 4—6 настоящей статьи Конференция государств-участников, если она сочтет это необходимым, учреждает любой соответствующий механизм или орган для содействия эффективному выполнению Конвенции.

Статья 79. Международная техническая комиссия

1. Конференция государств-участников в целях оказания содействия государствам в проведении обзора осуществления Конвенции создает и учреждает Международную техническую комиссию по противодействию преступности в сфере ИКТ (МТК).

2. МТК является постоянно действующим органом, состоящим из 23 членов, и формируется по смешанному принципу: две трети ее членов представляются Конференцией государств-участников, а одна треть — руководящими органами Международного союза электросвязи (МСЭ).

3. Члены Комиссии являются экспертами, обладающими непосредственным и значительным опытом в вопросах, касающихся дипломатии, международного и уголовного права, коммуникационных технологий или проведения соответствующих исследовательских разработок.

4. Члены Комиссии работают в течение пяти лет и могут назначаться повторно.

5. Сессии МТК созываются не реже одного раза в год в штабквартире МСЭ или Управления ООН по наркотикам и преступности или в таких местах и в такое время, которые могут быть указаны или утверждены Конференцией государств-участников.

6. Комиссия разрабатывает правила процедуры своей работы, подлежащие утверждению Конференцией государств — участников Конвенции.

7. Комиссия проводит оценку технического прогресса в области ИКТ.

8. МТК через Конференцию государств-участников докладывает о результатах своей работы государствам-участникам и заинтересованным международным организациям.

Статья 80. Секретариат

1. Генеральный секретарь Организации Объединенных Наций обеспечивает необходимое секретариатское обслуживание Конференции государств — участников Конвенции.

2. Секретариат:

a) организует сессии Конференции государств-участников и МТК и обеспечивает их необходимым обслуживанием;

b) оказывает государствам-участникам по их просьбе помощь в представлении информации Конференции государств-участников и МТК и

c) обеспечивает необходимую координацию с секретариатами других соответствующих международных и региональных организаций и механизмов.

Глава VII
Заключительные положения

Статья 81. Выполнение Конвенции

1. Каждое Государство-участник принимает в соответствии с основополагающими принципами своего внутреннего права необходимые меры, включая законодательные и административные меры, для обеспечения выполнения своих обязательств.

2. Каждое Государство-участник может принимать более строгие меры, чем меры, предусмотренные настоящей Конвенцией, для предупреждения преступлений в сфере ИКТ и борьбы с ними.

Статья 82. Урегулирование споров

В случае возникновения спора между государствами-участниками относительно толкования или применения настоящей Конвенции они стремятся урегулировать его посредством переговоров, согласительной процедуры или арбитража либо иными мирными средствами, согласованными сторонами спора.

Статья 83. Подписание, ратификация, принятие и утверждение

1. Настоящая Конвенция открыта для подписания всеми государствами — членами ООН.

2. Настоящая Конвенция также открыта для подписания региональными организациями экономической интеграции при условии, что по меньшей мере одно из государств — членов такой организации подписало настоящую Конвенцию в соответствии с пунктом 1 настоящей статьи.

3. Настоящая Конвенция подлежит ратификации, принятию или утверждению. Документы о ратификации, принятии, утверждении или официальном одобрении сдаются на хранение Генеральному секретарю Организации Объединенных Наций. Региональная организация экономической интеграции может сдать на хранение свой документ о ратификации, принятии, утверждении или официальном одобрении, если по меньшей мере одно из ее государств-членов поступило таким же образом. В этом документе о ратификации, принятии, утверждении или официальном одобрении такая организация заявляет о сфере своей компетенции в отношении вопросов, регулируемых настоящей Конвенцией. Такая организация также сообщает депозитарию о любом соответствующем изменении сферы своей компетенции.

Статья 84. Вступление в силу

1. Настоящая Конвенция вступает в силу на девяностый день после даты сдачи на хранение тридцатого документа о ратификации, принятии, утверждении или официальном одобрении. Для целей настоящего пункта любой такой документ, сданный на хранение региональной организацией экономической интеграции, не рассматривается в качестве дополнительных к документам, сданным на хранение государствами — членами такой организации.

2. Для каждого из государств или региональных организаций экономической интеграции, которые ратифицируют, принимают или утверждают настоящую Конвенцию после сдачи на хранение тридцатого документа о таком действии, настоящая Конвенция вступает в силу на тридцатый день после даты сдачи на хранение таким государством или организацией соответствующего документа или в дату вступления настоящей Конвенции в силу в соответствии с пунктом 1 настоящей статьи в зависимости от того, что наступает позднее.

Статья 85. Поправки

1. По истечении трех лет после вступления в силу настоящей Конвенции Государство-участник может предложить поправку и направить ее Генеральному секретарю Организации Объединенных Наций, который затем препровождает предлагаемую поправку государствам-участникам и Конференции государств — участников Конвенции в целях рассмотрения этого предложения и принятия решения по нему. Конференция государств-участников прилагает все усилия для достижения консенсуса в отношении каждой поправки. Если все усилия по достижению консенсуса были исчерпаны и согласие не было достигнуто, то в качестве крайней меры для принятия поправки требуется большинство в две трети голосов государств-участников.

2. В вопросах, входящих в сферу их компетенции, региональные организации экономической интеграции осуществляют свое право голоса согласно настоящей статье, располагая числом голосов, равным числу их государств-членов. Такие организации не осуществляют свое право голоса, если их государства-члены осуществляют свое право голоса, и наоборот.

3. Поправка, принятая в соответствии с пунктом 1 настоящей статьи, подлежит ратификации, принятию или утверждению государствами-участниками и соответствующими региональными организациями экономической интеграции.

4. Поправка, принятая в соответствии с пунктом 1 настоящей статьи, вступает в силу в отношении Государства-участника или региональной организации экономической интеграции через 90 дней после даты сдачи на хранение Генеральному секретарю Организации Объединенных Наций ратификационной грамоты или документа о принятии или утверждении такой поправки двумя третями голосов.

5. Когда поправка вступает в силу, она становится обязательной для тех государств-участников или региональных организаций экономической интеграции, которые выразили согласие быть связанными ею. Другие государства-участники продолжают быть связанными положениями настоящей Конвенции или любыми поправками, ратифицированными, принятыми или утвержденными ими ранее.

Статья 86. Оговорки

Каждое Государство-участник путем письменного уведомления на имя Генерального секретаря Организации Объединенных Наций при подписании или сдаче на хранение ратификационной грамоты или документа о принятии, одобрении или присоединении может заявить, что оно воспользуется правом сделать оговорку относительно применения настоящей Конвенции. Оговорки к статьям 15—17, 19—20, 22—26, пункту 11 статьи 47 не допускаются.

Статья 87. Пересмотр приложения

1. Любое Государство-участник может предлагать поправки к перечню международно-правовых документов, содержащемуся в приложении к настоящей Конвенции.

2. Секретариат проводит мониторинг вновь принимаемых международно-правовых документов, которые могут затрагивать сферу применения настоящей Конвенции, и выносит предложения о внесении изменений в приложение на рассмотрение очередной сессии Конференции государств-участников.

3. Предложения о внесении поправок должны касаться только вступивших в силу универсальных и региональных международно-правовых документов, касающихся непосредственно международной преступности.

4. Проекты поправок, предложенных в соответствии с пунктом 1 настоящей статьи, направляются Генеральным секретарем Организации Объединенных Наций государствам-участникам. Если одна треть или более государств-участников, ратифицировавших настоящую Конвенцию, уведомляет Генерального секретаря Организации Объединенных Наций в течение шести месяцев со дня направления проекта поправки о своих возражениях против вступления поправки в силу, такая поправка не вступает в силу.

5. В вопросах, входящих в сферу их компетенции, региональные организации экономической интеграции осуществляют свое право голоса согласно настоящей статье, располагая числом голосов, равным числу их государств-членов. Такие организации не осуществляют свое право голоса, если их государства-члены осуществляют свое право голоса, и наоборот.

6. Если менее одной трети от общего числа государств-участников, ратифицировавших настоящую Конвенцию, направляют свои возражения против вступления поправки в силу в адрес Генерального секретаря Организации Объединенных Наций в течение шести месяцев со дня направления проекта поправки, такая поправка вступает в силу в отношении государств-участников, не возражающих против нее, через 30 дней по истечении шести месяцев, предназначенных для внесения возражений.

7. На Конференции государств-участников поправка принимается большинством голосов в две трети от общего числа государств-участников, ратифицировавших настоящую Конвенцию. Такая поправка вступает в силу для государств-участников, выразивших согласие на применение данной поправки, через 30 дней со дня, следующего за днем принятия поправки.

8. Государство-участник, ранее возразившее против поправки, может изменить свое решение и уведомить депозитария о ее принятии. В таком случае данная поправка вступает в силу в отношении соответствующего Государства-участника через 30 дней со дня, следующего за днем, когда оно уведомило Генерального секретаря Организации Объединенных Наций о ее принятии.

Статья 88. Денонсация

1. Государство-участник может денонсировать настоящую Конвенцию путем направления письменного уведомления Генеральному секретарю Организации Объединенных Наций. Такая денонсация вступает в силу по истечении шести месяцев после даты получения уведомления Генеральным секретарем.

2. Региональная организация экономической интеграции перестает быть участником настоящей Конвенции, когда все государства — члены этой организации денонсировали настоящую Конвенцию.

Статья 89. Депозитарий и языки

1. Депозитарием настоящей Конвенции назначается Генеральный секретарь Организации Объединенных Наций.

2. Подлинник настоящей Конвенции, английский, арабский, испанский, китайский, русский и французский тексты которой являются равно аутентичными, сдается на хранение Генеральному секретарю Организации Объединенных Наций.

В УДОСТОВЕРЕНИЕ ЧЕГО нижеподписавшиеся полномочные представители, должным образом уполномоченные на то своими правительствами, подписали настоящую Конвенцию.

Приложение

1. Единая конвенция о наркотических средствах (Нью-Йорк, 30 марта 1961 г.);

2. Конвенция о преступлениях и некоторых других актах, совершаемых на борту воздушных судов (Токио, 14 сентября 1963 г.);

3. Конвенция о борьбе с незаконным захватом воздушных судов (Гаага, 16 декабря 1970 г.);

4. Конвенция о психотропных веществах (Вена, 21 февраля 1971 г.);

5. Конвенция о предотвращении и наказании преступлений против лиц, пользующихся международной защитой, в том числе дипломатических агентов (Нью-Йорк, 14 декабря 1973 г.);

6. Международная конвенция о борьбе с захватом заложников (Нью-Йорк, 17 декабря 1979 г.);

7. Конвенция о физической защите ядерного материала (Вена, 3 марта 1980 г.);

8. Конвенция о борьбе с незаконными актами, направленными против безопасности морского судоходства (Рим, 10 марта 1988 г.);

9. Конвенция Организации Объединенных Наций о борьбе против незаконного оборота наркотических средств и психотропных веществ (Вена, 19 декабря 1988 г.);

10. Международная конвенция о борьбе с бомбовым терроризмом (Нью-Йорк, 15 декабря 1997 г.);

11. Международная конвенция о борьбе с финансированием терроризма (Нью-Йорк, 9 декабря 1999 г.);

12. Международная конвенция о борьбе с актами ядерного терроризма (Нью-Йорк, 13 апреля 2005 г.).

Оглавление

Жданов Юрий Николаевич,
Кузнецов Станислав Константинович,
Овчинский Владимир Семенович

Кибермафия
Мировые тенденции и международное противодействие

Монография

Издание не подлежит маркировке
в соответствии с п. 1 ч. 2 ст. 1 ФЗ № 436-ФЗ

ООО «Юридическое издательство Норма»
109316, Москва, Волгоградский пр-т, 2
Тел. (495) 625-45-05. E-mail: norma@norma-verlag.com
Internet: www.norma-verlag.com

Редактор *М. Л. Шацкая*
Корректор *Л. А. Попенова*
Дизайн обложки *М. А. Агаркин*
Верстка: *Г. С. Брудовская*

Подписано в печать 00.00.22
Формат 60×90/16. Бумага офсетная
Гарнитура «Таймс». Печать цифровая
Усл. печ. л. 11,5. Уч.-изд. л. 9,34
Тираж 300 экз. Заказ №

По вопросам приобретения книг обращайтесь:

Отдел продаж «ИНФРА-М» (оптовая продажа)
127282, Москва, ул. Полярная, д. 31в, стр. 1
Тел.: (495) 280-15-96. Факс: (495) 280-36-29
E-mail: books@infra-m.ru

Отдел «Книга — почтой»
Тел.: (495) 280-15-96 (доб. 246)