В. С. Овчинский

Криминология цифрового мира

Учебник

2-е издание, дополненное и переработанное

НОРМА
ИНФРА-М
Москва, 2026

УДК 343.9::004.738.5(075.8)
ББК 67.51я73
О35

Автор

Владимир Семенович Овчинский — доктор юридических наук, заслуженный юрист РФ, советник министра внутренних дел РФ.

Рецензенты

А. Л. Осипенко — доктор юридических наук, профессор, заместитель начальника Краснодарского университета МВД России.
И. Ю. Сундиев — доктор философских наук, профессор.

Овчинский В. С.

О35 Криминология цифрового мира : учебник / В. С. Овчинский. — 2-е изд., доп. и перераб. — Москва : Норма : ИНФРА-М, 2026. — 348 с. — DOI 10.12737/2238805.

ISBN 978-5-00156-476-8 (Норма)
ISBN 978-5-16-021818-2 (ИНФРА-М, print)
ISBN 978-5-16-114567-8 (ИНФРА-М, online)

Учебник посвящен актуальным вопросам криминологического анализа преступности цифрового мира и мерам ее предупреждения.

Для магистрантов, специализирующихся в области криминологии и информационной безопасности.

УДК 343.9::004.738.5(075.8)
ББК 67.51я73

ISBN 978-5-00156-476-8 (Норма)
ISBN 978-5-16-021818-2 (ИНФРА-М, print)
ISBN 978-5-16-114567-8 (ИНФРА-М, online)

Содержание

Предисловие ко второму изданию

За годы, прошедшие после выхода первого издания учебника, проблема преступности цифрового мира приобрела еще бóльшую актуальность как в мире, так и у нас в стране. Главный показатель преступности цифрового мира — это киберпреступность.

В России в 2024 г. доля преступлений в сфере информационно-коммуникационных технологий (далее — ИКТ) составила 40% от общего числа зарегистрированных в стране. Такое значение стало максимальным в пятилетней статистике общего числа преступлений с 2020 г. Согласно данным Министерства внутренних дел РФ, за 12 месяцев 2024 г. зарегистрировано 765,4 тыс. киберпреступлений. Это на 13,1% превышает показатель 2023 г.

По данным Сбербанка, в 2025 г. совокупный ущерб от кибератак для экономики Российской Федерации приблизился к 1,5 трлн руб., более 53% российских компаний подверглись кибератакам. Каждая четвертая организация понесла значительные финансовые потери, а серьезные последствия от атак ощутили 80% пострадавших компаний. Четверть компаний признали, что столкнулись с существенными репутационными рисками. И почти половина отметили, что у них были простои, деятельность их бизнеса, сайтов приостанавливалась. Серьезные кибератаки на российские компании происходят каждые три минуты. Частота попыток взлома возрастает в три раза ежегодно.

Выступая на расширенном заседании коллегии МВД России 5 марта 2025 г., Президент России В. В. Путин обратил особое внимание на преступления, совершенные с использованием ИКТ. Поставлена задача искать новые, более эффективные методы борьбы с этой угрозой, в том числе в рамках единой системы противодействия подобным преступлениям. Такая система создается сейчас в соответствии с национальными целями развития России.

24 декабря 2024 г. Генеральная Ассамблея ООН консенсусом одобрила разработанную по инициативе России Конвенцию против киберпреступности (Конвенция ООН против киберпреступности; укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-

коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям).

Принятый документ — итог пятилетней кропотливой работы государств — членов ООН. Он стал первым в истории универсальным международным договором в области информационной безопасности, подтвердил востребованность новых норм международного права для справедливого регулирования цифровой сферы в интересах всего мирового сообщества.

Конвенция призвана стать прочной основой для налаживания правоохранительного сотрудничества в противодействии использованию ИКТ в преступных целях. Она нацелена на борьбу с несанкционированным доступом к электронным данным и их незаконным перехватом; подлогом, хищением или мошенничеством; отмыванием доходов от противоправных деяний; сексуальной эксплуатацией детей и надругательством над ними. Закрепляется цифровой суверенитет государства над своим информационным пространством, в том числе посредством наращивания международного взаимодействия между компетентными ведомствами. В перспективе сфера охвата соглашения может быть расширена за счет разработки протокола по дополнительным составам преступлений. В фокусе — борьба с использованием ИКТ в террористических и экстремистских целях, а также в торговле наркотиками и оружием.

Вне рамок Конвенции государства-участники могут осуществлять международное сотрудничество друг с другом в соответствии со своими международными обязательствами в любых других формах, допускаемых внутренним законодательством государства-участника, применимыми договорами о взаимной правовой помощи или эквивалентными соглашениями[1].

После выхода первого издания учебника автор самостоятельно и в соавторстве опубликовал по данной теме ряд книг[2]. В этот же период

[1] О вкладе России в разработку принятой Конвенции ООН см.: *Пузырева Ю. В., Бардина Е. Е., Мысина А. И.* и др. Противодействие использованию информационно-коммуникационных технологий в преступных целях: приоритеты международного сотрудничества РФ. М., 2024.

[2] См.: *Овчинский В. С.* Виртуальный щит и меч: США, Великобритания, Китай в цифровых войнах будущего. М., 2018; *Ларина Е. С., Овчинский В. С.* Криминал будущего уже здесь. М., 2018; *Они же.* Искусственный интеллект. Большие данные. Преступность. М., 2018; *Они же.* Искусственный интеллект. Этика и право. М., 2018; *Жданов Ю. Н., Овчинский В. С.* Полиция будущего. М., 2018; *Они же.* Киберполиция XXI века. Международный опыт. М., 2020; *Жданов Ю. Н., Кузнецов С. К., Овчинский В. С.* COVID-19: преступность, кибербезопасность, общество, полиция. М., 2020; *Они же.* Киберма-

в России были опубликованы монографии и учебные издания, развивающие проблемы, изложенные в нашем учебнике[1].

фия. Мировые тенденции и международное противодействие. М., 2022; *Ларина Е. С., Овчинский В. С.* Цифровая революция. Преимущества и риски. М., 2022; *Они же.* Искусственный интеллект: на войне, в разведке, борьбе с криминалом. М., 2025.

[1] См.: *Гилинский Я. И.* Неокриминология. Криминология постмодерна. СПб., 2025; *Бессонов А. А.* Изучение преступной деятельности с использованием искусственного интеллекта. М., 2025; *Он же.* Искусственный интеллект и математическая статистика в криминалистическом изучении преступлений. М., 2021; *Лебедев С. Я., Джафарли В. Ф.* Цифровое уголовное право. М., 2025; *Джафарли В. Ф.* Криминология кибербезопасности: в 5 т. / под ред. *С. Я. Лебедева*. М., 2021; *Русскевич Е. А.* Компьютерные преступления. Квалификационные алгоритмы и тренды: учеб. пособие. М., 2025; *Он же.* Уголовное право и «цифровая преступность»: проблемы и решения. М., 2022; Цифровое право: учебник. 2-е изд. / под ред. *В. В. Блажеева, М. А. Егоровой*. М., 2025; Цифровая криминалистика:учебник. 2-е изд. / под ред. *В. Б. Вехова, С. В. Зуева.* М., 2025; *Чурилов А. Ю.* Право новых технологий: учебник. 3-е изд. М., 2025; *Гайдамакин А. А.* Искусственный интеллект в юридической аналитике: учеб. пособие. М.; Вологда, 2025; Цифровое право: учебник / под ред. *Э. Л. Сидоренко.* М., 2024; *Колычева А. Н., Васюков В. Ф.* Расследование преступлений с использованием компьютерной информации из сети Интернет / под ред. *А. Г. Волеводза*. М., 2024; *Васюков В. Ф., Волеводз А. Г., Долгиева М. М.* и др. Преступления в сфере высоких технологий и информационной безопасности. М., 2023; *Дремлюга Р. И.* Преступность 4.0. Киберпреступность: вчера, сегодня, завтра. М., 2024; *Менисов А. Б.* Киберщит. Искусственный интеллект и кибербезопасность. М.; Алматы, 2024; *Шахназаров Б. А.* Право и информационные технологии в условиях современных трансграничных вызовов. М., 2024; *Николайчук И. А., Янгляева М. М., Якова Т. С.* Цифровое обществоведение. Медиа, метасмыслы, наука. М., 2023; *Киселева Л. С., Семенова А. А.* Цифровое общество: словарь-справочник. М., 2023; *Бахтеев Д. В.* Искусственный интеллект. Этико-правовые основы. М., 2023; *Евдокимов К. Н.* Противодействие технотронной преступности: теория, законодательство, практика. Иркутск, 2023; *Минаков С. С., Закляков П. В.* Информационные технологии и преступления (взгляд на цифровые следы со стороны следствия): учеб. пособие. М., 2023; *Арцимович Д. А.* Искусство цифровой самозащиты. М., 2023; *Гаврилов М. В., Климов В. А.* Информатика и информационные технологии: учебник. 5-е изд. М., 2023; *Нагродская В. Б.* Новые технологии (блокчейн/искусственный интеллект) на службе права: науч.-метод. пособие / под ред. *Л. А. Новоселовой*. М., 2023; *Ашманов И. С., Касперская Н. И.* Цифровая гигиена. СПб., 2022; *Куженелева-Саган И. П., Носова С. С., Спичева Д. И.* Цифровое общество-Сеть и его кочевники: учеб. пособие. Томск, 2022; *Барчуков В. К.* Информационное обеспечение, искусственный интеллект, правоохранительная деятельность. М., 2022; *Расторопов С. В., Барчуков В. К.* Мошенничество в сфере компьютерной информации: уголовно-правовой и криминологический аспекты. СПб., 2021; *Ищук Я. Г., Пинкевич Т. В., Смольянинов Е. С.* Цифровая криминология: учеб. пособие. М., 2021; *Полежаев О. А.* Право новых техологий: учеб. пособие / под ред. *Л. А. Новоселовой*. М., 2021; *Василенко Л. А., Мещерякова Н. Н.* Социология цифрового общества. Томск, 2021; *Залоило М. В.* Искусственный интеллект в праве. М., 2021; *Багмет А. Н., Бычков В. В., Скобелин С. Ю.* и др. Цифровые следы преступлений. М., 2020; *Бегишев И. Р., Бикеев И. И.* Преступления в сфере обращения цифровой информации. Казань, 2020.

Введение

Цифровой мир XXI в. — системное понятие, интегрирующее такие категории, как цифровая среда (пространство), цифровые технологии, цифровое общество, цифровая экономика, цифровое государство и граждане цифрового мира.

В 2025 г. Интернетом пользовались 5,56 млрд человек на планете, или 67,9% населения Земли, 96,3% из них подключались к Сети через мобильные устройства, 5,24 млрд человек имели аккаунты в социальных сетях.

Россия уже живет в цифровой эре: в 2025 г. 133 млн россиян ежедневно использовали Интернет — уровень его проникновения в России достигает 92,2%.

Важнейшим *критерием перехода* страны в цифровой мир является всеобщая связанность, интеграция личных девайсов (многофункциональных устройств), общественных сетей, корпоративных систем и правительственных инфраструктур в единое целое — цифровой взаимосвязанный мир. Это открывает невиданные возможности, но одновременно делает нас обитателями дома со стеклянными стенами. В таком случае возможности, риски и угрозы растут пропорционально и экспоненциально.

Данный факт требует кардинального *изменения подхода к национальной цифровой безопасности и кибербезопасности* как несущей конструкции цифровой безопасности.

Криминология цифрового мира представляет собой, с одной стороны, часть общей науки криминологии, на которую распространяется традиционное учение о причинах преступности, личности преступника, мерах предупреждения преступлений. С другой стороны, учитывая специфический характер самого цифрового мира, действующей в нем преступности и факторов, ее детерминирующих, криминология цифрового мира может рассматриваться как самостоятельная наука, предполагающая также и самостоятельную учебную дисциплину.

Актуальность такой учебной дисциплины весьма велика. Ее обусловливают:

Федеральный закон от 26 июля 2017 г. № 187-ФЗ «*О безопасности критической информационной инфраструктуры Российской Федерации*»;

Стратегия развития информационного общества в Российской Федерации на 2017—2030 годы, утв. Указом Президента РФ от 9 мая 2017 г. № 203;

Доктрина информационной безопасности Российской Федерации, утв. Указом Президента РФ от 5 декабря 2016 г. № 646;

Национальная стратегия развития искусственного интеллекта на период до 2030 года, утв. Указом Президента РФ от 10 октября 2019 г. № 490;

Государственная программа Российской Федерации «Информационное общество», утв. постановлением Правительства РФ от 15 апреля 2014 г. № 313;

Концепция государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий, утв. распоряжением Правительства РФ от 30 декабря 2024 г. № 4154-р (см. приложение 2);

План мероприятий по реализации Концепции государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий, утв. распоряжением Правительства РФ от 14 августа 2025 г. № 2207-р (см. приложение 3).

В учебнике рассмотрены понятие и элементы цифрового мира; технологии цифрового мира и криминогенные факторы, действующие в эпоху третьей и четвертой промышленных революций; особенности преступности, терроризма и экстремизма цифрового мира; личности преступников и преступные организации, действующие в цифровом мире; меры предупреждения преступлений в цифровом мире и роль в этом искусственного интеллекта.

Раздел I
ЦИФРОВОЙ МИР КАК ОБЪЕКТ КРИМИНОЛОГИЧЕСКОГО АНАЛИЗА

Глава 1. Элементы и содержание цифрового мира

§ 1. Цифровая среда (пространство)

Для целей данного учебника понятие *цифровой среды* (пространства) во многом идентично мировому пониманию *информационного пространства*, определяемого Стратегией развития информационного общества как совокупность информационных ресурсов, созданных субъектами информационной сферы, средств взаимодействия таких субъектов, их информационных систем и необходимой информационной инфраструктуры.

Что касается понятия *информационной инфраструктуры* России, то в учебнике используется определение, даваемое в Доктрине информационной безопасности. Это совокупность объектов информатизации, информационных систем, сайтов в сети Интернет и сетей связи, расположенных на территории России, а также на территориях, находящихся под юрисдикцией России или используемых на основании международных договоров России.

Информационная среда существует столько же, сколько существует человечество. Менялись лишь средства коммуникации, способы хранения и предоставления информации, уровень ее доступности.

Цифровое пространство представляет собой метафору, характеризующую пространство распространения сигналов в любых управляющих системах[1].

Очевидно, что цифровая среда (пространство) получила принципиально новое качество с появлением Интернета, базирующегося на информационных технологиях и электронно-вычислительной технике. В основе любых вычислений лежат операции с цифрами. Поэтому буквально в последние годы и в официальных выступлениях, и в публикациях, и в терминологии различных профессиональных сообществ,

[1] См.: *Ларина Е., Овчинский В.* Кибервойны XXI века. О чем умолчал Эдвард Сноуден. М., 2014.

включая политиков, военных, стратегистов и т. п., и в повседневном языке все чаще используется термин «цифровая среда».

Определяющим элементом для цифровой среды являются *цифровые технологии* (англ. digital technology). Цифровая технология в отличие от аналоговой работает с дискретными, а не с непрерывными сигналами.

Цифровые технологии главным образом используются в вычислительной цифровой электронике, прежде всего компьютерах, в различных областях электротехники, таких как игровые автоматы, робототехника, автоматизация, измерительные приборы, радио- и телекоммуникационные устройства и многие другие цифровые устройства.

Цифровая среда имеет собственные:

— инфраструктуру. Она включает в себя: телекоммуникационные и интернет-линии (оптоволоконные кабели и т. п.); вычислительные комплексы различной размерности — от суперкомпьютеров до смартфонов и планшетных компьютеров; вычислительные управляющие встроенные блоки в различного рода объекты физического мира, начиная от производственных линий и заканчивая кроссовками и майками, соединенными в цифровое пространство;

— структуру. Она состоит из сетевых программных протоколов, обеспечивающих передачу информации по различным сетям, включая Интернет, корпоративные сети, одноранговые сети (типа Tor); программ и программных платформ, осуществляющих хранение, переработку и предоставление информации — от баз данных до привычных всем операционных систем типа Windows, Linux; программ-интерфейсов, обеспечивающих восприятие информации конечными пользователями (интерфейсы сайтов, блогов, порталов, приложений, различного рода программ и т. п.);

— ультраструктуру. Она представляет собой инфосферу, где содержатся воспринимаемые человеком прямые и скрытые смыслы, выраженные в текстах, таблицах, видео- и аудиоконтенте. Ультраструктура включает в себя, во-первых, общедоступные сетевые ресурсы типа сайтов, блогов, порталов, социальных сетей и т. п., во-вторых, защищенные, доступные только для определенных категорий пользователей информационные ресурсы государственной и корпоративной принадлежности, в-третьих, общедоступные ресурсы с платным контентом.

За историю развития общедоступных коммуникационных сетей (с 1991 г.) сложилось два принципиально различных их типа:

1) *Интернет*, а также *внутренние государственные и корпоративные сети, недоступные для сторонних пользователей.* Эти сети построены по иерархическому принципу. В сетях существует несколько уровней иерархии, которые аккумулируют и передают информацию. Соответственно, права и возможности регулирования информации на каждом уровне зависят от положения в иерархии: чем выше уровень, тем больше возможностей и прав;

2) так называемые *пиринговые, или одноранговые, сети*[1]. Наиболее популярные из них в настоящее время — коммуникационная сеть Tor и платежная сеть Биткойн. В одноранговых сетях информация передается между компьютерами пользователей, которые имеют абсолютно равные права и возможности в передаче информации. В силу этого одноранговые сети работают, как правило, намного медленнее, чем Интернет.

Указанные типы сетей функционируют независимо друг от друга. Соответственно, ресурсы одной сети не обнаруживаются и не находятся поисковыми системами другой сети. При этом в каждой из сетей предусмотрены специальные порталы, которые облегчают использование ресурсов в другой сети.

Интернет имеет следующую *картографию*:

— *web 1.0.* Это наиболее старый, сложившийся сегмент Сети. Он включает в себя правительственные, корпоративные, общественные, персональные порталы, сайты, блоги, онлайн-СМИ. Ресурсы этого сегмента Сети легкодоступны при помощи поисковых систем (Google, Yandex и проч.);

— *web 2.0.* Это так называемый социальный веб, или веб социальных сетей и платформ. Здесь расположены такие ресурсы, как «ВКонтакте», Facebook[2], Twitter (с 2023 г. — X) и проч. Контент в этом сегменте Интернета создается в основном самими пользователями, поэтому он получил название *социального веба*. Из-за политики собственников платформ и социальных сетей, а также из-за требований приватности они лишь частично видимы для поисковых систем. В этом сегменте ускоренными темпами растет доля видео- и фотоконтента;

— *web 3.0.* Этот сегмент Интернета появился после 2010 г. и растет наиболее быстрыми темпами. Это так называемый *веб мобильных приложений*. Интерфейсы приложений размещаются на экранах планшетных компьютеров, смартфонов. Соответственно, пользователи рабо-

[1] Одноранговая, децентрализованная или пиринговая (от англ. peer-to-peer, P2P — равный к равному) сеть — это компьютерная сеть, основанная на равноправии участников.

[2] Принадлежит компании Meta, признанной экстремистской организацией и запрещенной в Российской Федерации.

тают с приложениями без обращения к поисковым системам, просто устанавливая связь между своим устройством и Интернетом;

— *невидимый Интернет*. Это ресурсы, которые не обнаруживаются поисковыми машинами, а также порталы, сайты и т. д., доступ к которым предполагает либо платный характер, либо наличие специального разрешения на использование ресурсов. По имеющимся данным, в невидимом Интернете находится около 90% всего ценного научно-технического, технологического, финансово-экономического и государственного открытого контента. Объемы невидимого Интернета постоянно растут. Он развивается более быстрыми темпами, чем web 1.0 и web 2.0. Главными причинами опережающих темпов являются, с одной стороны, стремление к архивации всех доступных данных корпоративными пользователями, а с другой — желание обладателей ресурсов вывести их из общедоступного пользования в платный сегмент, т. е. монетизировать;

— *Интернет вещей* (англ. Internet of things; далее — IoT). Представляет собой соединенные через Интернет с управляющими центрами встроенные информационные блоки самых различных объектов физического мира, в том числе производственной, социальной, коммунальной инфраструктуры. Например, к нему относятся подсоединенные к Всемирной сети технологические линии, системы управления водо- и теплоснабжением и т. п. В последние годы быстрыми темпами растет подключение к Интернету всех типов домашнего оборудования, бытовой техники, вплоть до холодильников, стиральных машин и т. п.;

— *бодинет* (англ. bodynet). Со стремительным развитием микроэлектроники появилась возможность встраивать элементы, передающие информацию, в предметы гардероба (кроссовки, майки и т. п.), а также широко использовать микроэлектронику в новом поколении медицинской техники, реализующей различного рода имплантаты — от чипов, контролирующих сахар в крови, до искусственного сердца и т. п. Кроме того, новой тенденцией стало создание *распределенного компьютера*, который предполагает, что отдельные его элементы распределяются по человеческому телу: фактически человек носит на себе компьютер и взаимодействует с ним круглые сутки.

Большую часть одноранговых сетей относят к так называемому *темному вебу* (англ. dark web). Своим названием этот сегмент Сети обязан широкому использованию своих ресурсов различного рода преступными, незаконными группами и группировками. Основными сегментами этого веба являются *сеть Tor*, созданная в 2002 г. военно-морской разведкой США, и *платежная сеть криптовалют*. В настоящее

время сети часто используются для противоправной деятельности, киберпреступности, торговли наркотиками, оружием, детской порнографией и т. п., а также для осуществления целенаправленных акций по подрыву государственного суверенитета.

Особый сегмент Сети, располагающийся частично в сети Интернет, частично — в специально созданных одноранговых сетях, составляют так называемые *сети денег*. Общемировой тенденцией является сокращение наличного платежного оборота и переход к электронным деньгам во всех их видах. Сеть денег включает в себя специализированные телекоммуникационные расчетные сети типа SWIFT, связывающие крупнейшие банки, а также платежные системы, использующие Интернет, типа PayPal, «Яндекс.Деньги» и т. п. Отдельным быстро развивающимся сегментом денежных сетей являются *специализированные платежные системы, базирующиеся на одноранговых сетях и зашифрованных сообщениях*. Наиболее известные из этих систем — платежные системы криптовалют.

Таким образом, цифровая среда имеет сложную картографию, где отдельные сегменты развиваются по собственным, независимым от общих закономерностей трендам. При этом ряд основополагающих тенденций являются общими для всех сегментов цифровой среды.

§ 2. Цифровой мир в эпоху третьей и четвертой промышленных революций

Цифровой мир сегодняшнего дня уникален и не имеет исторических аналогов, поскольку основывается сразу на *двух новых промышленных революциях*. В последние несколько лет в ведущих странах мира — от США до Китая, от Южной Кореи до Германии — разворачиваются и набирают темпы третья и четвертая промышленные революции. Третья стала предметом обсуждения ведущих мировых политиков, предпринимателей и экспертов после опубликования в 2011 г. международного бестселлера американского экономиста Дж. Рифкина «The Third Industrial Revolution: How Lateral Power Is Transforming Energy, the Economy, and the World»[1].

Новой производственной революции посвящены также два бестселлера 2012 г. — книги британского журналиста П. Марша «Новая промышленная революция: потребители, глобализация и конец массового производства» («The New Industrial Revolution: Consumers, Globalization

[1] См.: *Рифкин Дж.* Третья промышленная революция: как горизонтальные взаимодействия меняют энергетику, экономику и мир в целом. М., 2016.

and the End of Mass Production») и англо-американского писателя и предпринимателя К. Андерсона «Производители: Новая промышленная революция» («Makers: The New Industrial Revolution»).

В 2016 г. на Всемирном экономическом форуме в Давосе его председатель К. Шваб провозгласил начало четвертой промышленной революции. Вскоре после давосского форума в свет вышла книга К. Шваба, которая была переведена практически на все основные языки мира, «The Fourth Industrial Revolution»[1].

Под четвертую промышленную революцию в Германии реализуется программа «Индустрия-4.0».

В 2017 г. заговорили уже о пятой революции. В марте на выставке CeBit в немецком городе Ганновере (ключевом для мира инноваций мероприятии, объединившем в 2017 г. 200 тыс. человек и 3 тыс. технологических компаний) японский премьер-министр С. Абэ презентовал свой проект «Общество-5.0» (Society 5.0). Этот проект шел еще дальше, чем проект четвертой промышленной революции «Индустрия-4.0». Идея японских властей — поставить новые технологии на службу обществу, внедрить их во все сферы жизни. Цель — оптимизировать быт, деловую деятельность, эффективнее решать проблемы старения населения, ухода за людьми с ограниченными возможностями, обучения.

Промышленная революция означает глубокие, быстрые в исторической перспективе, скачкообразные (фазовые) изменения в самих основах техники и технологий, используемых во всех основных отраслях хозяйства. Эти изменения ведут к необратимым и качественным сдвигам в организации труда и производства, системах снабжения, маркетинга и потребления. Промышленная революция изменяет базовые структуры экономической жизни, полностью перестраивает социум и привычные способы его регулирования, преобразует политические институты.

Новые промышленные революции по своим масштабам, последствиям и сдвигам не только стоят наравне, но, возможно, и превосходят первую и вторую производственные революции[2].

Уже на начальных стадиях новых промышленных революций можно выделить несколько определяющих черт:

[1] См.: *Шваб К.* Четвертая промышленная революция. М., 2017.

[2] Как известно, первая производственная революция конца XVIII — начала XIX в. была связана с текстильной отраслью, энергией пара, углем, железными дорогами и т. п. Вторая производственная революция конца XIX — первой половины XX в. стала детищем электричества, двигателей внутреннего сгорания, триумфом машиностроения и конвейера как метода организации производства.

— одновременное широкое производственное применение различных независимых кластеров технологий, прежде всего робототехники, 3D-печати, новых материалов со спроектированными свойствами, биотехнологий, новых информационных технологий, и, конечно же, диверсификация энергетического потенциала производства и общества;

— постоянно возрастающее взаимодействие между отдельными технологическими кластерами, их своеобразное «слипание», взаимное кумулятивное и резонансное воздействие друг на друга;

— появление на границах технологических кластеров принципиально новых, не существовавших ранее технологий и семейств технологий, в которых кластеры взаимодействуют между собой.

Основа основ превращения отдельных технологических кластеров или паттернов в единую технологическую платформу — это *информационные технологии*. Они буквально пронизывают все стороны технологической и производственной жизни, связывая между собой отдельные технологические блоки. Наиболее яркими примерами этого являются такие технологические паттерны, как биотехнологии, робототехника, управляемая на основе больших данных, и т. п.

В сфере организации производства и труда отличительной чертой новых производственных революций является миниатюризация производства в сочетании с сетевой логистикой и персонификацией потребления продукции.

Децентрализация производства, переход к прямым связям в сфере распределения и персонификации потребления будет происходить в условиях сохранения господства цифровых гигантов, контролирующих ключевую технологию новой производственной революции — системы сбора, хранения, интеллектуальной обработки и распределенной доставки цифровых данных и компьютерных программ всех типов и размеров.

Первым ключевым направлением новых промышленных революций является *стремительная автоматизация и роботизация производства*, армии и всех сторон общественной жизни. Как отмечают эксперты, многие элементы автоматизации и роботизации могли быть внедрены в промышленное производство еще в 90-е гг. прошлого и первое десятилетие нынешнего века. Однако в те времена экономически выгоднее оказалось использовать вместо роботов практически дармовой труд рабочих из Китая и других азиатских стран. По прошествии времени ситуация изменилась. С одной стороны, труд в Азии заметно подорожал. С другой стороны, деиндустриализация Америки, многих стран Европы и частично Японии нанесла сильнейший удар по экономике этих стран. Наконец, в последние годы появились принципиально новые программ-

ные и микроэлектронные решения, позволяющие в разы повысить эффективность и функционал роботов при снижении себестоимости их производства. Сегодня, например, типовой американский робот на конвейере окупается в течение полутора — максимум двух лет.

Принципиально новые производства, линии и т. п. массово и согласованно приходят на смену традиционным технологиям, организационным структурам и финансово-экономическому механизму, характерному для индустрии второй производственной революции. Ключевую роль, без сомнения, играют робототехника, IT-технологии и биотехнологии.

Вторым направлением новых промышленных революций является *3D-печать*. В ее основе лежит технология Additive Manufacturing, т. е. аддитивное (можно сказать, поэтапное) изготовление. Метод подразумевает, что принтер послойно формирует изделие, пока оно не примет окончательный вид. 3D-принтеры не наносят на бумагу краску, а «выращивают» объект из пластмассы, металла или других материалов. В 2014—2016 гг. произошел прорыв в области промышленного использования 3D-печати крупнейшими корпорациями. Линии 3D-печати в настоящее время строят Boing, Samsung, Siemens, Canon, General Electric и др. Скорость и масштабы 3D-печати достигли рекордных показателей благодаря внедрению новых технологий (параллельная печать несколькими экструдерами и лазерное спекание с повышенной мощностью).

Третьим направлением новых промышленных революций является *производство новых материалов*, включая материалы с заранее спроектированными свойствами, композитные материалы и т. п. Необходимость появления широчайшей гаммы новых материалов диктуется, с одной стороны, требованиями широкого внедрения экономичной, эффективной 3D-печати, а с другой — развитием микроэлектроники, биотехнологий и т. п.

В свое время новое материаловедение связывали исключительно с *наноматериалами*, т. е. с новыми материалами, производимыми на основе миниатюризации.

Ключевым направлением новых промышленных революций являются, без сомнения, *биотехнологии* в широком смысле этого слова. По сути, сюда входит *индустрия индивидуализированных лекарств*, на которые делают ставку и фармацевтические гиганты, и новые, молодые, быстроразвивающиеся компании в этой сфере. Сюда же относятся различные виды *регенеративной медицины*. Широко используются *возможности 3D-печати для производства донорских органов*. Сегодня это уже не фантастика, а прошедшая клинические испытания обыденность, которую взяли на вооружение медицинские учреждения Франции, Германии, Соединенных Штатов, Израиля, Китая и других стран.

Особым направлением является *биоинформатика*. Группе исследователей во главе с американским ученым Дж. К. Вентерем удалось впервые в истории создать *искусственную жизнь*, используя ДНК одного из вирусов. Теперь эта команда может производить новые виды бактерий и живых организмов прямо из компьютера. Дж. Вентер так и заявил, что им удалось сделать «первый самовоспроизводящийся биологический вид на планете, родителем которого является компьютер».

Стержневой составляющей, пронизывающей все технологические кластеры новых промышленных революций и превращающей их в единый технологический пакет, являются, без сомнения, *информационные технологии*. В структуре информационных технологий выделяются три ключевые составляющие.

Первая — это *большие данные* (англ. big data). Большие данные — это сбор, хранение, оцифровка, обработка и предоставление в удобном для пользователя виде в любое время и в любой точке всей совокупности сведений о тех или иных событиях, процессах, явлениях и т. п. Ключевым в больших данных является то, что они позволяют работать именно со всей информацией в режиме он-лайн. Главным здесь является слово «всей». У пользователя больших данных имеется вся картина, не зависящая, как раньше, от каких-либо выборок, ограничений по источникам, времени предоставления данных и т. п. Большие данные могут включать в себя любые форматы — от таблиц до потокового видео, от оцифровки старых отчетов до текстовой записи, сделанной теми или иными источниками. Никогда раньше в истории человечества у лиц, занимающихся анализом, прогнозированием, конструкторско-инженерной деятельностью, геологией, принятием решений и т. д., не было возможности оперировать всей информацией. Причем не просто оперировать, а получать эту информацию в удобном и доступном для восприятия виде. Сегодня безусловными лидерами в сфере больших данных являются США, Великобритания, Япония и Китай. В этих странах имеются большое количество платформ, обеспечивающих работу с большими данными, специальные курсы подготовки, множество центров, где компании могут получить консультации или услуги, связанные с большими данными.

Сами по себе большие данные являются важнейшим государственным и корпоративным активом, который при должном использовании обеспечивает их владельцам устрашающее интеллектуальное превосходство и деловое доминирование.

Вторая ключевая составляющая — это *когнитивные вычисления и экспертные системы*. За последние годы Соединенным Штатам и Великобритании удалось осуществить подлинный прорыв в области создания экспертных систем, базирующихся на так называемых когнитивных вычислениях. В основу когнитивных вычислений заложены программы, моделирующие и имитирующие некоторые известные психофизиологические процессы. За счет этого созданы программы, которые обладают возможностями совершенствования, учитывающего при решении тех или иных задач ошибки.

Третья ключевая составляющая — это *облачные и распределенные вычисления*. Согласно российской Стратегии развития информационного общества облачные вычисления — информационно-технологическая модель обеспечения повсеместного и удобного доступа с использованием сети Интернет к общему набору конфигурируемых вычислительных ресурсов (облаку), устройствам хранения данных, приложениям и сервисам, которые могут быть оперативно предоставлены и освобождены от нагрузки с минимальными эксплуатационными затратами или практически без участия провайдера.

В период 2014—2025 гг. все ведущие страны мира приняли государственные документы, касающиеся в основном вопросов национальной безопасности. В них впервые зафиксирован важнейший вывод. *Любая высокая технология имеет тройное применение: гражданское, военное и криминальное*. Соответственно, новые промышленные революции в целом, их направления и конкретные технопакеты *не только открывают новые возможности, позволяют создать эффективные средства противодействия силам деструкции, но и наделяют преступников и террористов новыми, не существовавшими ранее методами и инструментами*. Одним из важнейших следствий этого процесса является подтверждение прогноза польского писателя-фантаста С. Лема, который в трактате «Summa Technologiae»[1] предсказал, что *по мере технологического прогресса неуклонно возрастает разрушительная мощь малых групп и даже отдельных индивидов*. В работе, изданной еще в начале 1960-х гг., Лем спрогнозировал, что в начале XXI в. маленькие группы террористов и бандитов и даже отдельные преступники смогут шантажировать и ставить под угрозу нормальное функционирование и жизнь населения мегаполисов и даже небольших государств. Новая производственная революция превратила этот прогноз в реальность.

[1] См.: *Лем С.* Сумма технологий. М., 2012.

§ 3. Цифровое (информационное) общество

Стратегия информационного общества понимает само это общество в широком смысле — как *общество, в котором информация и уровень ее применения и доступности кардинальным образом влияют на экономические и социокультурные условия жизни граждан*.

Международные принципы создания информационного общества и подходы к его созданию определены Окинавской хартией глобального информационного общества (2000 г.), Декларацией принципов «Построение информационного общества — глобальная задача в новом тысячелетии» (2003 г.), Тунисским обязательством (2005 г.).

В докладе Генерального секретаря ООН «Прогресс, достигнутый в осуществлении решений и последующей деятельности по итогам Всемирной встречи на высшем уровне по вопросам информационного общества на региональном и международном уровнях, включая ее 20-летний обзор» от 22 января 2025 г. содержится подробный анализ доступа к Интернету, роли искусственного интеллекта, управления цифровой сферой, проблемы информационной добросовестности.

Введение термина «информационное общество» приписывают профессору Токийского технологического университета Ю. Хаяши, который в 1969 г. по заказу правительства Японии опубликовал доклады: «Японское информационное общество: темы и подходы» и «Контуры политики содействия информатизации японского общества». В 1971 г. Токийский технологический университет представил публике доклад «План информационного общества». В этих работах говорилось о том, что компьютеризация обеспечит людям доступ к надежным источникам информации, освободит их от рутинной работы и создаст высокий уровень автоматизации производства. Производство не материального («индустриального»), а «информационного» продукта станет двигателем образования и развития нового, «информационного» общества.

В США принято считать, что понятие «информационное общество» ввел в науку в 50-х гг. прошлого века эмигрировавший в США австрийский экономист Ф. Махлуп. Он же говорил о наступлении эры «информационной экономики».

Если углубиться еще дальше в историю — в 40-е гг. XX в., можно найти записку англо-австралийского экономиста К. Кларка о перспективе появления «общества информации и услуг».

Американский социолог Д. Белл полагал, что информационное общество как следующая стадия общественного развития может характеризоваться тремя основными критериями:

1) должен произойти переход от доминирования индустриального производства к производству услуг (массовый рабочий не нужен);

2) научное знание приобретает определяющее значение в процессе реализации технологических нововведений;

3) интеллектуальные технологии должны стать ключевым элементом системного анализа и теории принятия решений[1].

В середине 1990-х гг. американский социолог испанского происхождения М. Кастельс выпустил трехтомную монографию «The Information Age»[2]. Исследование являет собой энциклопедический анализ роли и места информации в современном мире.

По мнению Кастельса, начиная с 70-х гг. прошлого века появляющиеся новые формы капитализма постепенно начинают оформляться в то, что автор называет *информационным капитализмом, главным ресурсом которого становятся информационные сети*, необходимые как для обеспечения производства внутри конкретного предприятия, так и для ведения бизнеса по всему миру.

§ 4. Цифровая экономика и ее технологии

Стержневой основой цифрового мира является *цифровая экономика*, которую Стратегия развития информационного общества определяет как хозяйственную деятельность, в которой ключевым фактором производства являются данные в цифровом виде, обработка больших объемов и использование результатов анализа которых по сравнению с традиционными формами хозяйствования позволяют существенно повысить эффективность различных видов производства, технологий, оборудования, хранения, продажи, доставки товаров и услуг.

Правительством РФ была сформирована национальная программа «Цифровая экономика Российской Федерации». Целями этой программы, утвержденной распоряжением Правительства РФ от 28 июля 2017 г. № 1632-р[3], являлись:

— создание экосистемы цифровой экономики РФ, в которой данные в цифровой форме являются ключевым фактором производства во всех сферах социально-экономической деятельности, обеспечено эффективное взаимодействие, включая трансграничное, бизнеса, научно-образовательного сообщества, государства и граждан;

— создание необходимых и достаточных условий институционального и инфраструктурного характера; устранение имеющихся препятствий и ограничений для создания и (или) развития высокотехнологических бизнесов и недопущение появления новых препятствий и ограничений как в традиционных отраслях экономики, так и в новых отраслях и на высокотехнологичных рынках;

— повышение конкурентоспособности на глобальном рынке как отдельных отраслей экономики России, так и экономики в целом.

Согласно Паспорту национального проекта «Национальная программа «Цифровая экономика Российской Федерации», утвержденному протоколом заседания президиума Совета при Президенте РФ по стратегическому развитию и национальным проектам от 4 июня 2019 г. № 7 в состав национальной программы входило девять федеральных проектов:

«Нормативное регулирование цифровой среды»;

«Информационная структура»;

«Кадры для цифровой экономики»;

«Информационная безопасность»;

«Цифровые технологии»;

«Цифровое государственное управление»;

«Искусственный интеллект»;

«Развитие кадрового потенциала IT-отрасли»;

«Обеспечение доступа в Интернет за счет спутниковой связи». Национальная программа завершена 31 декабря 2024 г.

Цифровая экономика представлена *тремя* следующими *уровнями*, которые в своем тесном взаимодействии влияют на жизнь граждан и общества в целом:

1) рынки и отрасли экономики (сферы деятельности), где осуществляется взаимодействие конкретных субъектов (поставщиков и потребителей товаров, работ и услуг);

2) платформы и технологии, где формируются компетенции для развития рынков и отраслей экономики (сфер деятельности);

3) среда, которая создает условия для развития платформ и технологий и эффективного взаимодействия субъектов рынков и отраслей экономики (сфер деятельности) и охватывает нормативное регулирование, информационную инфраструктуру, кадры и информационную безопасность.

Развитие цифровой экономики России основывается на трендах третьей и четвертой промышленных революций.

[1] См.: *Белл Д.* Социальные рамки информационного общества // Новая технократическая волна на Западе / отв. ред. *П. С. Гуревич*. М., 1986. С. 330—342; *Он же.* Грядущее постиндустриальное общество: опыт социального прогнозирования. М., 2001.

[2] См.: *Кастельс М.* Информационная эпоха: экономика, общество и культура. М., 2000.

[3] Утратило силу с 12 февраля 2019 г.

Полная оцифровка экономики. Сквозное проникновение технологий во все отрасли экономики как в качестве цифровых (нематериальных) активов в форме новых бизнес-моделей, так и в форме промышленного Интернета вещей обусловливает формирование больших массивов экономически значимых отраслевых и межотраслевых данных. Равно сквозное проникновение технологий в социальную сферу — в форме технологий связи и коммуникаций и Интернета вещей, когда практически каждый предмет быта и окружающего человека мира оказывается подключен к глобальному цифровому пространству, формирует предпосылки для использования соответствующих данных для оценки и прогнозирования экономического развития.

Обеспечение всеобщего доступного подключения к высокопроизводительным широкополосным сетям. Всеобщий доступ к Интернету позволит развивать преимущества Интернета вещей. По самым скромным подсчетам, к 2045 г. к Интернету по всему миру будет подключено более 100 млрд устройств. Это будут мобильные и переносные устройства, приборы, медицинские устройства, промышленные датчики, камеры безопасности, автомобили, одежда и др. Все эти устройства будут производить и обрабатывать огромное количество информации. Люди будут использовать информацию, полученную через IoT, для принятия более разумных решений, более глубокого понимания собственной жизни и окружающего мира. В то же время устройства, подключенные к Интернету, также автоматизируют многие задачи мониторинга, управления и ремонта, которые в настоящее время требуют человеческого труда. Пересечение IoT, аналитики и искусственного интеллекта создаст глобальную сеть умных машин, которые будут проводить огромное количество критически важных бизнес-операций без участия человека. Хотя IoT улучшит многие аспекты экономической эффективности, общественной безопасности и производительности труда, это также потребует дополнительных мер по обеспечению кибербезопасности и защиты конфиденциальности.

Цифровые платформы. В настоящее время существует множество цифровых платформ, которые обеспечивают рынки товаров, услуг и информации, поставляемых как в физическом, так и в цифровом виде.

Государственные цифровые платформы представляют собой цифровую экосистему, технологическую среду с API (англ. application programming interface — интерфейс программирования приложения), предоставляющую услуги и сервисы для управления жизненными ситуациями граждан, а также площадку, где формируются договоры между государством и различными категориями стейкхолдеров (от

англ. stake — доля и holder — держатель) — лиц или организаций, заинтересованных в получении государственных услуг. На государственных платформах могут предоставляться в том числе бесплатные сервисы, основанные на обработке открытых больших данных — как для бизнеса, так и для населения.

Компании-платформы — один из базовых элементов новой экономики. Следует наращивать инвестиции в национальные цифровые платформы. Развитие цифровых технологий должно быть включено во все программы и планы социально-экономического развития. Задействованным в развитии цифровых платформ частным компаниям должен быть обеспечен максимально облегченный доступ к кредитам, субсидиям, налоговым и иным финансовым льготам.

Инфраструктура для хранения информации. С учетом объема устройств, подключенных к цифровому пространству, и общей цифровизации экономики количество данных растет экспоненциально. В связи с этим возрастает роль высокотехнологичных решений для безопасного, надежного, долгосрочного хранения больших данных.

Технологии обработки больших данных. Для упрощения масштабного перехода бизнеса на цифровые платформы требуется снижение стоимости вычислительной мощности. Решения в данной сфере будут обусловливать конкурентные преимущества и уменьшать порог входа микробизнеса на рынок информационных услуг.

Формирование доверенного цифрового пространства. Формирование доверенной среды для хранения и обработки больших данных, а также для аутентификации и идентификации субъектов цифровой экономики в цифровом пространстве обусловит повышение уровня вовлеченности бизнеса и населения в цифровую экономику и обеспечит предоставление качественных цифровых услуг.

Новые технологии и их влияние на традиционные сектора экономики. Цифровые инновации в узком смысле относятся к внедрению нового или значительно улучшенного продукта информационно-коммуникационных технологий (товара или услуги), т. е. инновационной продукции в этой области; в широком смысле — к использованию ИКТ для внедрения нового или значительно улучшенного продукта, процесса, метода маркетинга или организационного метода, т. е. инноваций с использованием ИКТ.

Технологии, которые определяют переход к цифровой экономике. *Технологии в области работы с данными* включают:

— *искусственный интеллект* (далее — ИИ) — науку и технологию создания интеллектуальных машин, особенно интеллектуальных ком-

пьютерных программ; свойство интеллектуальных систем выполнять творческие функции, которые традиционно считаются прерогативой человека. Искусственный интеллект связан со сходной задачей использования компьютеров для понимания человеческого интеллекта, но не обязательно ограничивается биологически правдоподобными методами;

— *туманные вычисления* (англ. fog computing) — архитектуру системного уровня для расширения облачных функций хранения, вычисления и сетевого взаимодействия. Концепция предполагает обработку данных на конечных устройствах сети (компьютерах, мобильных устройствах, датчиках, смарт-узлах и т. п.), а не в облаке;

— *квантовые технологии* — технологии, в которых используются специфические особенности квантовой механики, прежде всего квантовая запутанность. Цель квантовой технологии состоит в том, чтобы создать системы и устройства, основанные на квантовых принципах, к которым обычно относят дискретность (квантованность) уровней энергии (квантово-размерный эффект, квантовый эффект Холла); принцип неопределенности Гейзенберга; квантовую суперпозицию чистых состояний систем; квантовое туннелирование через потенциальные барьеры; квантовую сцепленность состояний;

— *суперкомпьютерные технологии* — набор инструментов для решения специализированных задач с использованием специализированных вычислительных машин (суперкомпьютеров), которые превосходят по техническим параметрам и скорости вычислений большинство существующих в мире компьютеров. Суперкомпьютеры представляют собой большое число высокопроизводительных серверных компьютеров, соединенных друг с другом локальной высокоскоростной магистралью для достижения максимальной производительности в рамках подхода распараллеливания вычислительной задачи;

— *технологии идентификации* — автоматическую идентификацию и сбор данных — AIDC (англ. automatic identification and data capture) — общий термин для методов автоматической идентификации объектов, сбора данных о них и обработки данных автоматическими и автоматизированными системами. Технологии идентификации объектов включают магнитную карту, чип-карту, оптические (штрихкод, data matrix, OCR), радиочастотные (RFID, RTLS), биометрические (дактилоскопия in vitro, определение ДНК), аудиологические (распознавание голоса), оптические (идентификация по радужной оболочке глаза, распознавание лица) технологии;

— *математическое моделирование* — опосредованное практическое или теоретическое исследование объекта, при котором непосредственно изучается не сам интересующий нас объект, а некоторая вспомогательная искусственная или естественная система (модель), находящаяся в некотором объективном соответствии с познаваемым объектом, способная замещать его в определенных отношениях и дающая при ее исследовании в конечном счете информацию о самом моделируемом объекте;

— *сквозные технологии* — совокупность методов обработки, в составе которых на базе одной системы существует набор специализированных программ, не зависящих от конкретных методик и позволяющих осуществлять интерактивный обмен данными. Сквозная обработка — STP (англ. straight-through processing) — процесс непрерывной, полностью автоматизированной обработки информации. На всех этапах обработки данных исключено ручное вмешательство, что достигается применением стандартов обмена информацией между автоматизированными системами и их полного взаимодействия. Первичные данные могут формироваться как автоматическими системами, так и ручным вводом, но их последующая передача и обработка происходят полностью автоматически. В узком смысле STP-технология предполагает, что брокерская компания выступает в роли автоматического посредника между клиентами и внешним рынком. Ордера клиентов автоматически переправляются для заключения сделок на внешнем рынке или на крупного контрагента;

— *технологию блокчейна* — многофункциональные и многоуровневые информационные технологии, предназначенные для надежного учета различных видов активов[1]. Блокчейн (от англ. block — блок, модуль и chain — цепочка) — распределенная база данных, которая содержит непрерывно возрастающий набор упорядоченных записей (блоков), каждый блок содержит метку времени и связь с предыдущим блоком. Блокчейны — открытые, распределенные регистры, в которые могут вноситься записи о транзакциях между двумя участниками надежным и достоверным образом;

— *нейронные сети* — математические модели, а также их программные или аппаратные реализации, построенные по принципу организации и функционирования биологических нейронных сетей — сетей нервных клеток живого организма.

Технологии в области производства включают:

[1] См.: *Свон М.* Блокчейн: схема новой экономики. М., 2017; *Башир И.* Блокчейн: исчерпывающее руководство. М., 2025.

— *киберфизические системы* — CPS (англ. cyber-physical system) — системы, состоящие из различных природных объектов, искусственных подсистем и управляющих контроллеров, позволяющих представить такое образование как единое целое. Новизна и принципиальное отличие CPS от существующих встроенных систем или автоматизированных систем управления технологическим процессом, на которые они похожи внешне, состоит в том, что CPS интегрируют в себе кибернетическое начало, компьютерные аппаратные и программные технологии, качественно новые исполнительные механизмы, встроенные в окружающую их среду и способные воспринимать ее изменения, реагировать на них, самообучаться и адаптироваться;

— *3D-технологии (печать), или «аддитивное производство»,* — процесс создания цельных трехмерных объектов практически любой геометрической формы на основе цифровой модели. 3D-печать основана на концепции построения объекта последовательно наносимыми слоями, отображающими контуры модели. Фактически 3D-печать является полной противоположностью таких традиционных методов механического производства и обработки, как фрезеровка или резка, где формирование облика изделия происходит за счет удаления лишнего материала (так называемое субтрактивное производство);

— *роботизацию* — использование интеллектуальных робототехнических комплексов, функциональные особенности которых состоят в достаточно гибком реагировании на изменения в рабочей зоне;

— *аддитивные технологии* — технологии по созданию объектов за счет нанесения последовательных слоев материала. Модели, изготовленные аддитивным методом, могут применяться на любом производственном этапе — как для изготовления опытных образцов (быстрое прототипирование), так и в качестве самих готовых изделий (быстрое производство). В производстве, особенно машинной обработке, термин «субтрактивные» подразумевает более традиционные методы и является ретронимом, придуманным в последние годы для разграничения традиционных способов и новых аддитивных методов. Хотя традиционное производство использует по сути «аддитивные» методы на протяжении веков (такие, как склепка, сварка и привинчивание), в них отсутствует трехмерная информационная технологическая составляющая. Машинная же обработка (производство деталей точной формы), как правило, основывается на субтрактивных методах — опиловке, фрезеровании, сверлении и шлифовании;

— *технологии открытого производства* — технологии, основанные на новой модели социоэкономического производства, в рамках которой физические объекты создаются исходя из принципов открытости, взаимодействия и распределения, при этом модель основывается на принципах открытого проектирования и открытого источника (англ. open source).

Технологии в области взаимодействия с окружающей средой включают:

— *беспилотные технологии* — комплекс, оборудованный системой автоматического управления, который может передвигаться без участия человека;

— *безбумажные технологии* — технологии, при которых основным носителем информации является не бумажный, а электронный документ, формируемый на машинном носителе (в памяти компьютера) и доводимый до пользователя через экран дисплея;

— *мобильные технологии* — комплекс методов и решений (приложений, устройств), позволяющих достигать независимости пользователя от стационарных вычислительных устройств при решении поставленных задач;

— *биометрические технологии* — набор инструментов идентификации отдельно взятого человека, основанный на измерении его уникальных характеристик;

— *технологии «мозг — компьютер»* — нейрокомпьютерный интерфейс (НКИ), или прямой нейронный интерфейс, мозговой интерфейс, интерфейс «мозг — компьютер» — систему, созданную для обмена информацией между мозгом и электронным устройством (например, компьютером). В однонаправленных интерфейсах внешние устройства могут либо принимать сигналы от мозга, либо посылать ему сигналы (например, имитируя сетчатку глаза при восстановлении зрения электронным имплантатом). Двунаправленные интерфейсы позволяют мозгу и внешним устройствам обмениваться информацией в обоих направлениях. В основе нейрокомпьютерного интерфейса часто используется метод биологической обратной связи.

Цифровая трансформация сельского хозяйства. Для предотвращения глобальных вызовов в сфере продовольственной и биологической безопасности человечеству необходимо сельское хозяйство нового типа, соответствующее модели циркулярной (безотходной) экономики и принципам устойчивого развития. Вопросам перехода к новой экономической модели и к «интеллектуальному» сельскому хозяйству как ее неотъемлемому компоненту уделяют все большее внимание ведущие международные организации и национальные правительства.

Электронная торговля. Электронная торговля составляет значимый институт цифровой экономики, проникает во все большее количество правоотношений, складывающихся в сфере торговли, и охватывает весь спектр отношений — прямое взаимодействие потребителей с потребителями (англ. consumer-to-consumer, C2C), взаимодействие продавцов с потребителями (англ. business-to-consumer, B2C), взаимодействие между предпринимателями (англ. business-to-business, B2B), взаимодействие бизнеса и государства в электронной форме (англ. business-to-government, B2G) и др.

Цифровая трансформация в сфере связи и телекоммуникаций. По мере развития цифровой (электронной) экономики нагрузка на цифровую инфраструктуру, в основе которой лежат средства связи и телекоммуникаций, многократно возрастает. Пользователями востребуется уже не столько связь, сколько доступ к различным платформам, сервисам и услугам в электронном виде. Само понятие «пользователь» кардинально меняется, поскольку в условиях цифровой трансформации в эту категорию попадают не только люди, но и представители Интернета вещей (подключенные устройства), количество которых уже превышает количество людей в разы, а скоро превысит на порядки. Таким образом, речь идет о нагрузках на средства связи и телекоммуникаций и их пропускной способности, превосходящих существующие на несколько порядков.

Цифровая трансформация транспорта и логистики. «Цифровая логистика» возникает как ответ на глобальные вызовы цифровой экономики для традиционного сектора транспорта и логистики, такие как стремительно изменяющаяся глобализированная и сверхконкурентная торговая среда, сложность цепочек поставок, быстрое изменение ожиданий клиентов, ограниченные ресурсы инфраструктуры.

Проблемы логистики в электронной торговле связаны прежде всего с более быстрыми темпами формирования и реализации цепочек поставок товаров по сравнению с традиционной торговлей. Данная особенность электронной торговли определяет необходимость совершенствования механизмов прогнозирования спроса, что должно способствовать более рациональному планированию запаса товаров на складах в различных географических регионах, сокращая время оборота товаров и стоимость доставки. В рамках развития электронной торговли необходимо разрабатывать и внедрять технологии анализа данных по спросу для планирования распределительной логистики.

В то же время в секторе B2B перспективным может оказаться внедрение технологий, в том числе использующих достижения Интернета вещей, позволяющих потенциальному заказчику самостоятельно отслеживать актуальную информацию о предложении, а именно о готовящемся к реализации товаре, через отслеживание производственного цикла (факт изготовления, отгрузки, транзитное время, ориентировочная дата прибытия на склад и т. п.), что позволит осуществлять более эффективное планирование закупок и, соответственно, их логистическое обеспечение.

Сфера финансовых услуг. Под областью финансовых технологий понимают применение инновационных технологий в целях оказания финансовых услуг. Однако в связи со множеством применяемых в финансовой отрасли технологий границы термина «отрасль финансовых технологий» размыты.

Основными сегментами области финансовых технологий на данный момент являются: платежи и переводы, краудфандинг (от англ. crowd — толпа, funding — финансирование), управление активами, финансовый маркетплейс (англ. marketplace — рыночная площадь; в интернет-коммерции это место, где могут договариваться, заключать контракты участники рынка), блокчейн.

При этом мы видим усиление тенденции по созданию полностью цифровых банков, которые в своей деятельности ориентируются преимущественно на тех, кто предпочитает использование онлайн банковских услуг.

Цифровая трансформация энергетики. Россия является одним из крупнейших в мире производителей ископаемого топлива, в то же время запасы нефти и газа небезграничны и необходимы новые решения для создания высокоинтегрированных интеллектуальных системообразующих и распределительных электрических сетей нового поколения в Единой энергетической системе России (интеллектуальные сети — smart grid).

Цифровая трансформация ЖКХ. По прогнозам, к 2045 г. в городах будет жить 65—70% населения земного шара — примерно 6,4 млрд человек. Массовая миграция в города окажет значительное давление на городские транспортные системы, продовольствие и водоснабжение, энергетическую инфраструктуру, санитарию и общественную безопасность.

Информационные и коммуникационные технологии будут способствовать росту «умных городов», использующих данные и автоматизацию для увеличения эффективности и устойчивости городских центров. Распределенные сенсорные системы будут контролировать

потребление воды и электроэнергии и автоматически балансировать распределение по смарт-сетям. Сетевые системы трафика и автономные варианты транспортировки смогут революционизировать массовый транспорт и логистику. Новые материалы и методы проектирования будут использоваться для построения интеллектуальных зданий, которые максимизируют эффективность нагрева, охлаждения и освещения. Внешние солнечные панели, микроветряные турбины, тепловая энергия и другие возобновляемые источники энергии обеспечат чистую распределенную выработку электроэнергии.

Новые системы управления. В условиях цифровой экономики данные становятся формой капитала. Формирование, накапливание и использование такого рода капитала требуют тесного сотрудничества государства и бизнеса, государства и гражданского общества, бизнеса и гражданского общества. Однако экономические преимущества получают те государства и хозяйствующие субъекты, которые имеют не только доступ к данным, но также эффективные технологии их обработки. Качественный рост экономики возможен при наличии технологий, позволяющих максимально возможно точно оценивать текущее состояние рынков и отраслей, а также осуществлять эффективное прогнозирование их развития и быстро реагировать на изменения в конъюнктуре национальных и мировых рынков.

Основными принципами управления как на уровне промышленных предприятий, так и на уровне государства становятся:

— получение данных в реальном времени;

— управление экономическими процессами, основанное на автоматизированном анализе больших данных;

— высокая скорость принятия решений, изменение правил в реальном времени — мгновенное реагирование на изменения и интерактивность среды;

— ориентация на конкретного пользователя, жизненные ситуации клиентов как бизнес-процесс (пользователь становится ближе благодаря мобильным устройствам и Интернету вещей);

— решения в одно касание;

— цифровая экосистема как центр синергии государства, бизнеса и граждан.

Ключевым фактором успеха в цифровой экономике, высококонкурентной и трансграничной, становятся не технологии, а новые модели управления технологиями и данными, позволяющие осуществлять оперативное реагирование и моделирование будущих вызовов и проблем для государств, бизнеса и гражданского общества.

§ 5. Граждане цифрового мира и их права

Digital native примерно можно перевести как «коренной житель цифрового общества, человек, родившийся в цифровом обществе, цифровое поколение»[1].

Человек в цифровом обществе, его проблемы — это предмет междисциплинарных профессиональных интересов специалистов в области философии, информатики, психологии, лингвистики, медицины, этнографии, педагогики, экономики, а также связывающих эти дисциплины областях (таких, например, как психолингвистика или клиническая психология) и, конечно, криминологии.

В современном цифровом обществе особенно острым является *соблюдение прав граждан* при пользовании цифровыми технологиями.

«Государства должны содействовать доступу к Интернету как к общественной службе, с тем чтобы каждый человек независимо от своего места проживания мог пользоваться его благами». Такое требование содержится в проекте Кодекса этики для информационного общества (ЮНЕСКО, 2010 г.)[2].

В этом же рекомендательном документе сказано:

— там, где общий доступ пока обеспечить невозможно, государства должны предоставить всем людям возможность получать легкий доступ к Интернету, например с помощью телецентров, библиотек, общинных центров, больниц и школ. Люди должны получить доступ к разветвленной национальной системе интернет-услуг, подключенной к международной сети;

— создание телекоммуникационной инфраструктуры, разработка правил, определение платы, введение налогов и установление тарифов должны обеспечивать доступ для всех имущественных групп населения, при этом особое внимание следует уделять потребностям государственных служб, образовательных учреждений, обездоленных групп населения и инвалидов;

— необходимо разрабатывать интерфейсы, контенты и прикладные программы, которые обеспечивали бы доступ для всех, включая лю-

[1] Термин был предложен М. Пренски, американским писателем и популяризатором технологий обучения и просвещения, в статье «Digital Natives, Digital Immigrants» (2001 г.).

[2] См.: *Болгов Р. В., Еременков А. А., Чернов С. И.* Подходы международных организаций к защите прав человека в цифровом пространстве // Россия в глобальном мире. 2025. Т. 28. Вып. 1. С. 7—29.

дей с физическими, сенсорными или когнитивными недостатками, а также людей, говорящих на языках меньшинств;

— государства должны соответствующим образом содействовать применению открытых и технических стандартов взаимодействия программного и компьютерного обеспечения в цифровом мире, включая стандарты, разработанные для цифрового вещания, которые обеспечили бы людям широкий доступ к контенту;

— необходимо обеспечивать свободный доступ к информации для всех лингвистических групп, внедрять технологии, которые делали бы информацию доступной для людей с физическими недостатками, представителей обоих полов, лиц с разными уровнями развития, пожилых людей и групп, представляющих разные культуры и имеющих разный уровень дохода;

— люди должны иметь свободный доступ ко всей информации, представленной им другими. Люди должны иметь также удобные инструменты, позволяющие им легко, быстро и эффективно производить информацию, обмениваться ею и получать к ней доступ. Информационные сети должны быть открыты для контента из всех источников, что позволило бы всем заинтересованным лицам стать создателями продукции, а не оставаться лишь ее потребителями;

— государствам следует предотвращать попытки ограничить доступ и права на использование информации. Им следует обеспечить признание и осуществление права на всеобщий онлайновый доступ к общественной и правительственной документации, включая информацию, необходимую для граждан в современном демократическом обществе;

— государствам следует содействовать обеспечению доступа к ИКТ и образованию, чтобы позволить всем людям, особенно детям, приобрести и сохранить навыки, необходимые для работы с самыми разными ИКТ, и критически оценить качество информации, особенно той, которая могла бы причинить им вред;

— государства обязаны защищать свободу выражения мнений. Им следует содействовать свободе выражения мнений и свободе распространения информации не только как ценности самой по себе, но и как ценности, обеспечивающей осуществление других прав, таких как право на образование, право на уважение человеческого достоинства, право на свободу вероисповедания и т. д.;

— право на свободу выражения мнений не должно ограничиваться правительствами, за исключением лишь тех случаев, которые строго определены и регламентированы общепризнанными положениями

международного права или стандартами. Эти ограничения должны соответствовать международным правовым документам и стандартам по правам человека и принципам законности, а также устанавливаться соразмерно поставленной цели;

— государствам не следует подвергать интернет-контент каким-либо особым ограничениям, которые превышают ограничения, уже применяемые в отношении других средств распространения контента;

— органы власти не должны лишать общественность доступа к информации и другим коммуникационным продуктам в Интернете путем общей блокировки или фильтрации информации независимо от границ. Это не мешает установке фильтров для защиты малолетних, особенно в таких доступных для них местах, как школы или библиотеки, или для защиты Интернета от таких эндогенных угроз, как вирусы, вредоносные программы, спам и другие вредные технологии;

— государствам следует принять соответствующие нормам международного права законодательные акты, направленные на защиту личных данных и частной жизни, защиту пользователей от незаконного хранения их личных данных, защиту от хранения неточных личных данных или от злоупотребления ими, от несанкционированного разглашения таких данных, защиту от вторжения в их частную жизнь путем, например, произвольной рассылки сообщений с явными коммерческими целями;

— государствам следует уважать волю пользователей Интернета не разглашать свои личные данные и обеспечивать, чтобы ИКТ не использовались для слежки или контроля органами власти или частными структурами сверх того, что разрешено международными актами по правам человека. Это не мешает государствам принимать меры и сотрудничать с целью нахождения лиц, ответственных за преступные деяния, в соответствии с национальным законодательством и международными соглашениями, касающимися правосудия и полиции;

— государствам следует содействовать принятию регламентов, определяющих меры по самостоятельному и совместному регулированию участниками частного сектора деятельности по защите права на уважение частной жизни и охране тайны переписки;

— государственные или частные организации, требующие от отдельных людей предоставления личных данных, должны запрашивать лишь минимально необходимое количество таких сведений и на минимально короткий срок. Собранные данные должны быть за-

щищены от несанкционированного разглашения, а ошибки, связанные с угрозой личной безопасности, должны исправляться немедленно. В тех случаях, когда данные, собранные с определенной целью, больше не востребованы, они должны уничтожаться. Людей необходимо предупреждать о возможности использования представленных сведений не по назначению. Организации обязаны извещать людей в случае злоупотреблений, потери или кражи этой информации;

— государствам следует признать свободу граждан критиковать государственные или общественные учреждения. Критике со стороны средств массовой информации могут подвергаться государственные, правительственные или любые другие учреждения исполнительной, законодательной или судебной власти;

— государствам и другим заинтересованным сторонам следует сотрудничать в области повышения безопасности Интернета и информации, что дало бы им возможность пресекать действия, подрывающие их стабильность и наносящие ущерб наличию, достоверности, целостности и конфиденциальности сохраняемых или передаваемых данных и услуг, предлагаемых сетями и системами или открывающих доступ к ним;

— необходимо содействовать разработке общих правил сотрудничества между провайдерами услуг информационного общества и правоохранительными органами, обеспечивая среди прочего, чтобы такое сотрудничество осуществлялось строго на правовой основе, обеспечивающей соблюдение всех правил, регулирующих частную жизнь;

— государствам следует укреплять потенциал всех пользователей, включая детей и молодежь, с целью содействия обеспечению безопасного использования Интернета и ИКТ, недопущения появления и распространения незаконных и пагубных контентов путем регулирования в соответствии с международными стандартами;

— людям необходим свободный доступ к эффективным и действенным механизмам решения проблем, связанных с нарушениями прав человека. Когда права человека и основные свободы ставятся под угрозу материалами Интернета или же незаконным контролем, ограничениями свободы выражения мнений и других прав, участники должны иметь доступ к механизмам, позволяющим им принимать ответные меры по таким нарушениям.

Глава 2. Криминогенные факторы, действующие в эпоху четвертой промышленной революции[1]

§ 1. Социальное и цифровое неравенство

В теории криминологии с момента ее возникновения в XIX в. неравенство относили к числу главных причин преступности.

С начала XXI в. во всем мире слово «неравенство» не сходит со страниц газет и экранов телевизоров, по этой теме ежегодно публикуются тысячи книг и статей — как академических, так и публицистических. Большинство авторов полагают, что экономическое неравенство — это главное зло, с которым сталкиваются современные общества. Ведущие международные организации — Всемирный банк, Международный валютный фонд, Международная организация труда — заказывают и публикуют десятки специальных исследований, с разных сторон рассматривающих феномен экономического неравенства. В оборот вводятся все новые статистические данные о распределении доходов и богатства. С невероятной быстротой множится число посвященных этой проблеме научных работ. Книги о неравенстве становятся мировыми бестселлерами[2]. Многие видят в радикальном сокращении неравенства единственно возможный способ оживить экономический рост. Ожесточенные дебаты по этой проблеме ведутся сегодня и в России.

Для криминологов интерес представляет особый вид неравенства современного мира — *цифровой барьер, цифровое неравенство, информационное неравенство* (англ. digital divide) — ограничение возможностей социальной группы из-за отсутствия у нее доступа к современным средствам коммуникации.

Цифровой барьер является термином социально-политического характера. На возможности ущемленной группы влияют отсутствие доступа или ограниченный доступ к телевидению, Интернету, телефонной связи (мобильной и стационарной), радио. Все это ограничивает возможности этой группы в поиске работы, налаживании социальных связей, культурном обмене и может негативно влиять на экономическую эффективность, развитие и сохранение культуры, уровень образования. Согласно общепринятым воззрениям на цифровое (информационное) общество его специфика такова, что свободный обмен ин-

[1] Перечисляя подобные факторы, автор во многом основывается на выводах докладов Интерпола и Европола 2015—2025 гг. и ряда международных исследований (ООН, ЮНЕСКО, МВФ, Всемирного банка и др.).

[2] См., например: *Пикетти Т.* Капитал в XXI веке. М., 2015.

формацией способствует преодолению нищеты и неравенства, однако у тех, кто отключен от такого обмена, перспективы катастрофически ухудшаются.

Глобальный тренд заключается в том, что информационная экономика подключает к своей сети тех, кто представляет для нее ценность (тем самым придавая им дополнительную ценность), но отключает тех, кто не имеет для нее ценности (тем самым уменьшая их шансы обрести какую-то ценность)[1].

Не так важно, какими конкретно причинами продиктовано наличие цифрового неравенства между теми, кто может пользоваться благами и соблазнами Сети, и остальным миром. Существенно другое: *цифровое будущее провоцирует возникновение «новых бедных»*.

В эту группу можно зачислять не только тех, кто по объективным причинам лишен доступа к Интернету и цифровым устройствам. Сюда же попадают и пользователи, некачественно применяющие предложенные технические возможности. Кажется, что разница между этими группами велика, но это не совсем так. Первые не могут познакомиться с плодами научно-технической революции, вторые — осознанно или нет — не хотят. Результат в обоих случаях плачевен: будущее наступает без них.

Пока это расслоение может быть не столь заметным. В конце концов, многие из перечисленных технологических решений еще не стали продуктами, которые можно легко приобрести в ближайшем магазине. А какие-то рынки (например, нейротехнологий), несмотря на сопровождающий их большой медийный шум, еще только формируются. Но не надо быть футурологом, чтобы заметить: цифровые технологии завоевывают все большее внимание исследователей, становятся частью значительного количества самых разных экономических, политических, социокультурных инициатив и постепенно начинают обеспечивать жизнедеятельность не только частных лиц, но и сообществ, индустрий.

§ 2. Безработица в результате новых технологических революций

Безработица, как и неравенство, также всегда была основополагающим фактором преступности. Новая технологическая революция усугубила безработицу и падение доходов, устранив нужду в малопрофессиональных рабочих. Робототехника и сложное компьютеризированное оборудование успешно заменили квалифицированную рабочую силу. Искусственный интеллект и программное обеспечение теперь заменяют журналистов, создавая новости в электронном виде путем сканирования Интернета, трейдеров на финансовых рынках заменяют автоматизированные алгоритмы.

[1] См.: *Химанен П., Кастелс М.* Информационное общество и государство благосостояния: финская модель. М., 2002.

Коммуникации, сделавшие возможной недорогую передачу голоса, а также почти мгновенные трансферы огромных объемов данных наряду со все более высокочеткими изображениями способствовали перемещению производительных мощностей. Все возрастающими темпами это развивается в таких сферах, как инженерное дело, архитектура, бухгалтерский учет, юридические услуги и даже медицинские услуги.

В сочетании с технологией удаленного управления, изначально разрабатывавшегося для военных, теперь стало возможным контролировать высокоавтоматизированное производство и даже добычу в удаленных регионах.

Многим категориям работающих независимо от профессии и навыков сейчас угрожает *технологическая безработица*.

Существовала убежденность в том, что новые отрасли вберут в себя оставшихся без работы людей. Реальность оказалась иной. В 2025 г. мировые рынки труда продолжали ощущать эффект «второй волны» сокращений, запущенной в технологическом секторе в конце 2022 г. Несмотря на общее оживление экономики после пандемии COVID-19, спрос на разработчиков программного обеспечения и программистов демонстрирует заметное снижение как в США, так и во всем мире.

Основной драйвер этого тренда — все более активная интеграция инструментов ИИ и автоматизации в процессы разработки. По данным ресурса Indeed, в начале 2025 г. число вакансий для программистов упало на 35% по сравнению с 2020 г. Издание Business Insider также отмечает, что количество объявлений о вакансиях к 2025 г. сократилось на треть, в основном из-за того, что ИИ берет на себя разработку рутинных участков кода.

Сложность и динамизм цифровой экономики означают, что возможность трудоустройства для переучивающихся людей не гарантирована. Для тех, кто нашел работу, угроза неполной занятости или безработицы является постоянной, что затрудняет выстраивание долгосрочных планов и достижение долгосрочной финансовой и личной безопасности.

Хотя и существуют хорошо оплачиваемые места для небольшой части рабочей силы с необходимыми навыками, большинство новых ра-

бочих мест находится в секторе низкооплачиваемых услуг, таких как розничная торговля или безопасность. Молодежная безработица остается на высоком уровне.

Большая часть населения в настоящее время являются членами так называемого *уязвимого пролетариата* (термин, используемый в Японии для работников без гарантии занятости), которые составляют до 30% всех трудозанятых страны на фоне того, что компании сокращают издержки на рабочую силу.

Изменения на рынке рабочей силы влияют на характер общества. В новом цифровом мире совсем немногочисленная элита — 5% населения обладают существенными накоплениями и контролируют бóльшую часть ресурсов. Они нанимают еще один слой людей — 20%, чтобы управлять делами элиты, а также контролировать уязвимый пролетариат, который составляет 75% населения.

§ 3. Нарастание миграционных процессов негативного свойства

Миграция сохранит высокие темпы в течение следующих двух десятилетий. Люди ищут экономические возможности, бегут от конфликтов и ухудшающихся условий окружающей среды. Число международных мигрантов достигло самых высоких показателей в 2015 г. — 310 млн человек. Получается, что один из 112 человек в мире — это мигрант. К 2025 г. этот показатель несколько снизился. Но, по оценкам экспертов, рост числа иммигрантов и беженцев продолжится из-за глобальной экономической дифференциации, постоянных конфликтов и усиливающейся этнической и религиозной напряженности. Число мигрирующих людей сохранится на высоком уровне или даже увеличится из-за ухудшения экологических условий в предстоящие 20 лет.

В XXI в. масштабы законных и незаконных миграционных потоков являются крупнейшими за весь исторический период. В настоящее время существуют три ярко выраженных центра, привлекающих легальных и нелегальных мигрантов. Это Россия, Соединенные Штаты Америки и страны Европейского союза (ЕС). В каждом из отмеченных регионов свои закономерности, причины и формы нелегальной миграции.

При наличии некоторых общих черт ситуация с нелегальными мигрантами в России, США и странах ЕС существенно различается в настоящее время и будет различаться в ближайшее десятилетие.

Сразу после распада СССР численность нелегальных мигрантов в Россию из новых государств постсоветского пространства ежегодно возрастала. Поскольку двумя основными сферами занятости нелегальных мигрантов являются строительство и жилищно-коммунальное хозяйство, при экономическом оживлении стоит ожидать нового *увеличения численности нелегальных мигрантов*.

В первом полугодии 2025 г. в Россию въехало 5,48 млн граждан Узбекистана, Казахстана, Таджикистана, Китая и Кыргызстана — всего на 2% меньше, чем за аналогичный период 2024 г. Однако статистика по странам изменилась: если число мигрантов-таджиков сократилось на 150 тыс., то поток мигрантов из Китая и Казахстана вырос. По данным ФСБ России, больше всего приезжих прибыло из Узбекистана (1,82 млн), при этом большинство указали целью визита работу. Граждане Китая чаще приезжают как туристы (317 тыс.), а казахи — в частном порядке (около 1 млн).

Эксперты отмечают, что ужесточение миграционного законодательства (включая биометрический контроль и ограничение пребывания до 90 дней в течение года) пока не привело к значительному снижению потока.

По данным Следственного комитета РФ, с января по май 2025 г. число преступлений в России, которые совершили мигранты, выросло на 10% в сравнении с аналогичным периодом 2024 г. и превысило 18,8 тыс. Доля таких деяний в общем криминальном массиве увеличилась с 4,3% до 5%. Количество дел против мигрантов, направленных в суды, выросло на 15%.

Фигурантами дел стали почти 12,5 тыс. мигрантов. Вместе с ростом числа нарушений вырос объем преступлений повышенной общественной опасности. Число половых посягательств выросло на 22%, рост особо тяжких преступлений мигрантов составил 57% (до 6 тыс.).

Негативной тенденцией миграции иностранных граждан является их *вовлечение в криминальную террористическую среду*. К категории этих лиц прежде всего относятся иностранные граждане:

— участники международных террористических и экстремистских организаций;

— члены организованных групп и преступных сообществ.

Еще один фактор угрозы — *массовая вербовка* нелегалов эмиссарами ИГИЛ[1] и других радикальных группировок. Осуществляется это в основном через социальные сети.

[1] Запрещенная в России террористическая группировка.

Характерным примером взаимосвязи мигрантов и терроризма является теракт в «Крокус Сити Холле» (Красногорск, Московская область), который произошел 22 марта 2024 г. около 20:00 по московскому времени. Нападавшие открыли огонь по находившемуся в здании гражданскому населению, подожгли зрительный зал, а затем покинули здание и скрылись на автомобиле. В ходе атаки погибли 149 человек (из них шестеро детей) и 609 человек получили ранения. В результате взрывов и пожара здание концертного зала было почти полностью разрушено.

Ответственность за теракт взяло на себя афганское отделение международной террористической организации ИГИЛ[1] — «Вилаят Хорасан». Задержано более 10 человек в России, в том числе четыре предполагаемых исполнителя. Все четверо — граждане Таджикистана.

Интерпол и Европол регулярно публикуют подробные доклады, анализирующие процессы нелегальной миграции в тесной увязке с организованной преступностью и терроризмом. В последние годы беспрецедентного уровня достиг поток нелегальных мигрантов в Европейский союз. Это в основном люди, изгнанные из родных земель нестабильностью, отсутствием безопасности и ужасающей бедностью, породившими серьезный гуманитарный кризис и создавшими многочисленные возможности для транснациональных преступных сетей.

Организованным преступным группам (далее — ОПГ) выгоден приток миллионов мигрантов из стран Африки, Ближнего Востока и Азии, они извлекают криминальную прибыль, эксплуатируя потребность людей в помощи, их мечты о лучшей жизни. Мигрантам обеспечивают незаконное пересечение морских и сухопутных границ, изготовление и предоставление поддельных проездных документов и удостоверений личности, что создает сложности для правоохранительных органов в противодействии незаконной миграции.

По оценкам Европола, более 90% мигрантов, прибывающих в ЕС, используют *услуги, оказываемые преступными сетями.* В основном эти услуги связаны с транспортировкой и обеспечением размещения в стране пребывания; в большинстве случаев они предоставляются преступными группами, и криминальный бизнес получает все возрастающую прибыль, связанную с нелегальным ввозом мигрантов.

Благоприятно расположенные вдоль маршрутов горячие точки, совпадающие с транспортными хабами, привлекают мигрантов и используются контрабандными сетями. Горячие точки располагаются

[1] Запрещенная в России террористическая группировка.

в районах с развитой транспортной инфраструктурой, включая международные вокзалы, аэропорты, порты, точки технического обслуживания для междугородних автобусов и т. п. Наряду с транспортными хабами горячие точки возникают в районах со слабым контролем со стороны правоохранительных органов, а также в разрушенных или несостоявшихся государствах. Кроме того, горячие точки расположены в зонах пограничного контроля, особенно в тех местах, где криминальным сетям удалось коррумпировать пограничников, полицейские патрули и подразделения военно-морского флота. Горячие точки расположены также в местах расселения диаспор, сходных по этническому и национальному составу с незаконными мигрантами.

Преступные сети, организующие и обслуживающие незаконную миграцию, вытянуты вдоль миграционных маршрутов. Лидерами ОПГ являются в основном граждане стран, не входящих в ЕС, имеющие то же происхождение или вероисповедание, что и мигранты. При этом в состав сетей входят и граждане государств — членов ЕС. За пределами ЕС участники преступных сетей, как правило, работают с мигрантами того же этнического происхождения, что и они сами.

Фактически преступные сети авансируют незаконных мигрантов, поскольку транспортные услуги, а также продвижение по маршруту предполагают предварительные затраты. Преступные сети выступают как своеобразные кредитные учреждения по отношению к мигрантам. Оборотной стороной этого является жесткий контроль миграционного потока на всех его стадиях со стороны преступников с наличием в каждой мигрантской группе контролеров и своего рода охранников, обеспечивающих доставку мигрантов до места назначения в целости.

Данные Европола и Интерпола свидетельствуют: преступный бизнес на незаконной миграции все теснее сращивается с криминалом, специализирующимся на незаконном обороте наркотиков, подделке документов, имущественных преступлениях и торговле людьми и органами.

С географической точки зрения маршруты нелегальной миграции идентичны криминальным логистическим цепочкам, используемым для контрабанды товаров, а также наркотиков, оружия и т. п. В результате группы контрабандистов и наркосиндикаты включаются в бизнес, связанный с нелегальной миграцией. Кроме того, сам нелегальный интенсивный антропоток (перемещение людей) позволяет увеличить наркотрафик, объемы незаконной торговли оружием, контрабанду различных товаров и т. п.

Нелегальные мигранты уязвимы для криминальных сетей как до, так и после их прибытия в ЕС. В результате сложившихся условий, а также в силу необходимости оплатить транзит они подвергаются сексуальной эксплуатации со стороны преступных сетей, вынуждены работать на предприятиях криминальной экономики либо на легальных предприятиях без регистрации, с минимальной оплатой, перевозить наркотики, а также участвовать в качестве исполнителей самого низового уровня в деятельности преступных сетей, в том числе связанных с нелегальной миграцией.

В России с августа 2025 г. Московский многофункциональный миграционный центр разрабатывает систему на основе ИИ для автоматизации процессов предварительной проверки электронных версий документов иностранных граждан.

Система предназначена для полностью автоматической проверки комплектов документов, направляемых иностранными гражданами через Интернет и другие каналы связи. Она будет обрабатывать сканированные копии документов, необходимых для получения разрешения на временное проживание, вида на жительство, гражданства России, статуса носителя русского языка, а также для прохождения обязательной дактилоскопической регистрации, медицинского освидетельствования и подачи уведомлений о трудовой деятельности.

Ключевыми целями проекта являются исключение участия оператора в процессе проверки, расширение перечня онлайн-услуг и повышение скорости и качества обработки документов. Система будет интегрирована с существующей информационной системой многофункционального миграционного центра по электронной проверке документов (ИС ЭПД) через API-интерфейсы.

Архитектура системы построена по трехуровневому принципу и включает уровень хранения данных, уровень бизнес-логики и уровень представления. Классификация документов должна осуществляться с точностью не менее 98%, распознавание текста — также не менее 98%.

Для обучения нейронных сетей создается аннотированная выборка из не менее чем 8000 уникальных изображений для каждого типа документа. Производительность системы должна обеспечить обработку до 250 тыс. документов в сутки, время отклика — не более 10 секунд в штатном режиме и 180 секунд при пиковой нагрузке.

Работы выполняются в два этапа. На первом этапе создается основная функциональность системы, включая механизмы взаимодействия, распознавания, проверки и обучения нейросетей на 12 основных типах документов, таких как миграционная карта, заграничные паспорта различных стран, медицинские заключения и др. На втором этапе планируется дообучение системы для работы с дополнительными типами документов, включая патенты, полисы ДМС, свидетельства о рождении и иные правовые документы.

В качестве серверной операционной системы используется Windows Server 2012 и Ubuntu Server 16.04.7 и выше. Управление базами данных осуществляется с помощью системы управления базами данных PostgreSQL 16 или аналогичных решений, обеспечивающих реляционную или объектно-реляционную модель данных, поддержку многопроцессорной архитектуры и механизмов контроля целостности.

Клиентская часть системы будет функционировать в веб-браузере «Яндекс Браузер» версии 22.7.3 и выше, что соответствует модели «тонкого клиента». Для разработки программных решений используются языки программирования высокого уровня, включая Java 8 и C#.

В системе шесть основных подсистем: загрузки графических данных, распознавания текста документа, интеллектуальной проверки документов, формирования и отображения результатов, хранения данных и взаимодействия с внешними системами.

Каждая подсистема реализует строго определенный функционал, начиная с конвертации файлов различных графических форматов (PNG, JPEG, BMP, TIFF, PDF) в единый формат и заканчивая комплексным анализом документов с использованием статистических методов и нейросетевых моделей архитектуры трансформеров с механизмами внимания.

Для обеспечения взаимодействия с внешними системами, в частности с ИС ЭПД, разрабатываются API-интерфейсы, использующие протоколы HTTP/HTTPS и формат обмена данными XML. Интеграционные решения предусматривают возможность использования вебсервисов или обмена структурированными файлами специализированных форматов.

С 1 сентября 2025 г. в Москве и Московской области введено обязательное использование приложения «Амина» для мигрантов. Этот цифровой сервис предназначен для иностранных граждан, прибывающих в Россию без визы для трудовой деятельности.

Мигранты должны самостоятельно установить это приложение. Для авторизации в приложении потребуется действующая карта иностранного гражданина, которую можно оформить в миграционном центре. Если карта будет утеряна, авторизация возможна по паспортным данным.

§ 4. Новые технологии, международные и внутригосударственные конфликты

В следующие десятилетия могут нарастать риски возникновения конфликтов, в том числе межгосударственного характера. Риск возникновения конфликтов увеличится из-за расхождения интересов ведущих держав, увеличения террористической угрозы, длительной нестабильности в слабых государствах и распространения смертельных, разрушительных технологий. Разрушающиеся общества и несостоявшиеся государства станут распространенным явлением. Они будут обладать высокоточным оружием дальнего радиуса действия, кибер- и роботосистемами для проникновения в целевые инфраструктуры издалека и более доступными технологиями для создания оружия массового уничтожения.

Все чаще конфликты будут происходить не на поле боя, а в киберпространстве, финансово-экономической и ментальной сферах. Хроническая угроза загрязнения воздуха, нехватка воды и изменение климата станут более заметны. Это приведет к серьезным столкновениям. Между крупными державами, элитами и населением будет все меньше согласия в вопросах о путях решения глобальных и региональных проблем. Такая динамика развития неизбежно приведет к сбоям системы глобального управления.

Конфликты будет порождать не только соперничество между крупными державами, но и их увлечение гибридными и прокси-войнами (англ. proxy — представитель), т. е. опосредованными войнами, ведущимися чужими руками. В межгосударственных конфликтах все шире будут участвовать частные военные компании, иррегулярные воинские образования, рекрутируемые из бывших военных и криминала и т. п.

В условиях, когда небольшие террористические, повстанческие и преступные группы смогут иметь на вооружении технологии массового поражения, может возникнуть уникальная ситуация, отбрасывающая мир в Средневековье, когда с бандами преступников и отрядами наемников воевали государства. Эта тенденция уже проявляет себя. Количество, интенсивность, человеческие и экономические издержки конфликтов неуклонно растут начиная с 2011 г.

Военный конфликт на Украине, война в Газе, война Израиля и США против Ирана — наглядное подтверждение растущего напряжения.

Принципиальной чертой следующих десятилетий будет стирание граней между военными и невоенными инструментами, войной

и миром, юридическими нормами, применимыми в мирной и военной жизни. Более того, в ходе таких конфликтов стираются четкие грани между повстанцами, преступниками и террористами. Это становится огромной проблемой для всех крупных держав.

Будущие конфликты предполагают расширение сферы противоборств. Противоборства будут происходить не только в военной и дипломатической, но и в информационной, психологической, экономической и технологической сферах. В будущих конфликтах более слабая сторона предпочтет максимально уклоняться от традиционных военных действий и сосредоточивать свои усилия на террористических атаках против мирного населения и разрушении критической инфраструктуры противника. Инициаторы конфликта будут уходить во все более глубокое подполье.

Война в физическом пространстве по своему характеру приблизится к войне в киберпространстве. Идеалом для инициаторов подобных конфликтов будет ситуация, когда невозможно разобрать, кто, зачем и против кого воюет.

Для инициаторов конфликтов нового типа главным инструментом станет целенаправленное стравливание между собой этнических, религиозных, культурных, экономических и политических групп и их максимальное раздробление. Данная технология позволяет нарушить инфраструктуру общественного сотрудничества, которая является основой функционирования любого государства, возможно не менее важной, чем сама государственная власть. Такая стратегия направлена на максимальное обезличивание инициаторов при минимизации их расходов и перекладывании их на население и различного рода группы внутри страны — поля конфликта.

Подрывные группы. Негосударственные группы, в том числе террористы, боевики, преступные группировки, будут иметь все более широкий доступ к все более разнообразному спектру летальных и нелетальных средств огневого, инфраструктурного и поведенческого поражения. Уже сегодня такие группы получили доступ к самому современному вооружению и широкому спектру технологий. Это не только противотанковые ракеты, ракеты класса «земля — земля», дроны, но и современные виды программно-аппаратных средств информационного и поведенческого воздействия. Ранее такие вооружения были монополией государственных армий. Есть основания полагать, что неконтролируемая диффузия вооружений будет продолжаться.

Дополнительным фактором станет повсеместная доступность кибервооружений, которые уже сегодня могут нанести ущерб, превосхо-

дящий разрушения, вызванные огнестрельным оружием. Появление у деструктивных группировок все более разрушительных вооружений неизбежно будет побуждать государства и коалиции к превентивным, опережающим действиям против них. Это, в свою очередь, начнет раскручивать спираль конфликта, циклы насилия и придавать им все более идеологический характер, вплоть до религиозных войн.

Удаленные войны. Господствующей тенденцией конфликтов нового типа станет стремление государств и негосударственных акторов вести так называемые *неопознанные войны*, предполагающие дистанционные действия. Дистанционные атаки будут осуществляться как комбинация кибератак, использования высокоточного оружия, роботизированных систем и беспилотного оружия с применением средств поведенческого и психологического воздействия.

Дистанционные атаки ведут к снижению порога для начала конфликта. В то же время войны как обмен дистанционными атаками ломают равновесие между мечом и щитом. В удаленных войнах гораздо большее, чем в обычных, преимущество получает тот, кто атакует первым. Конфигурация конфликтов такого типа в решающей степени будет зависеть от того, способна ли одна из сторон конфликта не позволить другой навязать обычные военные действия, может ли она перенести военные действия на территорию напавшей страны. В связи с этим, несмотря на кажущийся менее кровопролитным характер войн издалека, они имеют гораздо больший, чем традиционные войны, потенциал неуправляемой эскалации. Кроме того, в таких войнах даже на первом этапе неизбежно будут задействованы не только воинские подразделения, но и террористические сети и даже никому не подчиняющиеся повстанческие отряды, сформированные из бывших преступников, или преступные группы, называющие себя повстанческими отрядами.

Будущие кризисы неизбежно будут иметь гораздо больший эскалационный потенциал и меньшую управляемость, чем традиционные войны, поскольку стороны — инициаторы конфликта будут иметь равные стимулы, чтобы нанести удар первыми, до того, как они подвергнутся нападению.

В удаленной войне целями первого порядка станут телекоммуникации и, соответственно, спутниковые группировки, их поддерживающие.

Проблема нового оружия массового поражения. Потенциально самой большой угрозой миропорядку является использование в качестве оружия достижений *биотехнологий и синтетической биологии*.

Эти технологии практически недоступны для международного контроля в его сегодняшнем виде, а по разрушительной мощи не уступают ядерному вооружению. Имеются данные, что овладеть подобного рода оружием стремятся террористические организации и преступные группировки.

В ближайшие два десятилетия вполне возможен крах слабых государств, обладающих определенной научной базой, в том числе на территории Европы и Центральной Азии. Это может открыть террористам и преступникам путь в лаборатории и к специалистам, способным произвести оружие массового поражения. Кроме того, возможна несанкционированная передача террористам и преступникам оружия массового поражения из государственных арсеналов этих слабых и несостоявшихся государств.

Конфликты в «серых» зонах. Размывание грани между войной и миром, между армиями национальных государств, частными военными компаниями и различного рода иррегулярными формированиями, между полноценными военными действиями, спецоперациями и террористическими актами, между непосредственными войнами и прокси-конфликтами меняет динамику современного мира. Чем дальше, тем больше эта разница будет стираться. Многие силы в современном мире заинтересованы в последовательном расширении «серой» зоны конфликтов. Их наиболее точным определением будет являться состояние «ни войны, ни мира». (Как известно, впервые этот термин применил Л. Троцкий при заключении Брестского мира.)

Характерной чертой конфликтов в «серых» зонах является изменение соотношения между летальными и нелетальными компонентами конфликта. На протяжении всей истории сердцевиной, кульминацией конфликта выступало применение летального оружия. Именно это подчеркивало высказывание «Война — это продолжение политики иными средствами».

В ближайшие 20 лет наряду с традиционными военными конфликтами все бóльшую роль будут играть конфликты, где применение летальных вооружений окажется вспомогательным компонентом, а основное противоборство будет происходить в финансово-экономической, технологической, информационной, поведенческой, экологической сферах и, конечно же, в киберпространстве.

В 2025 г. в Израиле раскрыли подробности уникальной государственной разработки под названием «Горизонт» — комплекса систем на основе ИИ, созданных для раннего выявления глобальных тенден-

ций и возможных мировых кризисов. Задача лаборатории стратегического прогнозирования, действующей в Министерстве инноваций, науки и технологий Израиля, — своевременно давать правительству сигналы о надвигающихся процессах и помогать адаптировать государственную политику в восьми сферах — от идеологии и демографии до международных отношений, экономики и геополитики. Соответственно этому «Горизонт» объединяет несколько платформ: одна из них отслеживает социальные и политические тренды, другая — технологические, третья анализирует цепочки поставок, а четвертая, самая сложная, пока остается в разработке.

Раздел II
ПРЕСТУПНОСТЬ ЦИФРОВОГО МИРА

Глава 3. Киберпреступность

§ 1. Международно-правовое определение киберпреступности

В многочисленных научных исследованиях предпринимаются попытки определить термин «киберпреступность». При анализе практически 200 актов национального законодательства, указанных странами в ответах на вопросник Всестороннего исследования проблемы киберпреступности, проведенного ООН в 2013 г., менее чем в 5% случаев термин «киберпреступность» присутствовал в названии или содержании правовых норм. Вместо этого в законодательстве чаще употребляются термины «компьютерные преступления», «электронные средства связи», «информационные технологии» или «преступления в сфере высоких технологий». На практике многие из этих законодательных актов определяют преступления, которые включены в понятие киберпреступности, например несанкционированный доступ к компьютерным системам или воздействие на компьютерные системы либо данные. В тех случаях, когда в национальном законодательстве слово «киберпреступность» все же присутствовало в названиях законодательных актов или разделов, в разделе, в котором давались определения, редко присутствовало определение этого термина. Если же правовое определение термина «киберпреступность» и получило закрепление в законодательстве, как правило, оно представляет собой просто отсылку к «преступлениям, определенным в настоящем Законе».

На 10-м Конгрессе ООН по предупреждению преступности и обращению с правонарушителями (Вена, 2000 г.) в ходе семинара на соответствующую тематику были выработаны два определения. *Киберпреступность в узком смысле* (компьютерная преступность) — это любое противозаконное поведение в форме электронных операций, направленное против безопасности компьютерных систем и обрабатываемых ими данных. *Киберпреступность в широком смысле* (преступления, связанные с применением компьютеров) — это любое противозаконное поведение, осуществляемое посредством или в связи с компью-

терной системой или сетью, включая такие преступления, как незаконное владение, предложение или распространение информации посредством компьютерной системы или сети.

Одно общепринятое определение описывает киберпреступность как любое деяние, в котором инструментом, целью или местом преступных действий являются компьютеры или сети. Такое широкое определение вызывает ряд трудностей. Например, относится ли к киберпреступности убийство, если правонарушитель использовал клавиатуру для того, чтобы нанести жертве смертельный удар?

В некоторых определениях просматриваются попытки учесть цели или намерения: киберпреступность определяется как действия, осуществляемые посредством компьютеров, которые либо являются незаконными, либо считаются противоправными некоторыми сторонами и которые могут быть совершены с помощью глобальных электронных сетей. Эти более точные описания исключают случаи, когда физическое оборудование используется для совершения обычных преступлений, но они таят риск исключить преступления, которые считаются киберпреступлениями в международных соглашениях, например в Конвенции Совета Европы о компьютерных преступлениях (2001 г.).

Что касается международных или региональных правовых документов, то лишь немногие из них предлагают определение киберпреступности. Например, ни в Конвенции Совета Европы о компьютерных преступлениях, ни в Конвенции о борьбе с преступлениями в области информационных технологий Лиги арабских государств (2010 г.) нет определения термина «киберпреступность» для целей этих документов. В Соглашении о сотрудничестве государств — участников Содружества Независимых Государств (СНГ) в борьбе с преступлениями в сфере компьютерной информации (2001 г.) не используется термин «киберпреступность», а дается определение «преступления в сфере компьютерной информации», представляющего собой «уголовно наказуемое деяние, предметом посягательства которого является компьютерная информация». Аналогичным образом в Соглашении о сотрудничестве в области обеспечения международной информационной безопасности между правительствами государств — членов Шанхайской организации сотрудничества (2009 г.) понятие «информационная преступность» определяется как «использование информационных ресурсов и (или) воздействие на них в информационном пространстве в противоправных целях».

В Конвенции Совета Европы о компьютерных преступлениях используются термины «компьютерная система» и «компьютерные данные». В проекте Конвенции Африканского союза также используются термины «компьютерная система» и «компьютерные данные». Решение ЕС об атаках на информационные системы содержит термины «информационная система» и «компьютерные данные». В Конвенции Лиги арабских государств используются термины «информационная система» и «данные», а в Соглашении Содружества Независимых Государств — термин «компьютерная информация».

Современный понятийный аппарат и классификация киберпреступлений подробно даются в Конвенции ООН против киберпреступности (2024 г.) (см. приложение 1).

§ 2. Периоды развития киберпреступности

Международный союз электросвязи в исследовании 2014 г. предлагает рассматривать следующие этапы.

В *1960-е гг.* появление транзисторных компьютерных систем, которые были меньше по размеру и дешевле по сравнению с ламповыми вычислительными машинами, привело к более широкому использованию компьютерных технологий. На этом раннем этапе правонарушения сводились к физическому повреждению компьютерных систем и накопленных данных. О подобных случаях сообщалось, например, в Канаде, где в 1969 г. студенческие беспорядки привели к пожару, в результате которого были уничтожены данные, хранившиеся в университете. В середине 1960-х гг. в США начались дебаты по поводу создания центрального учреждения по хранению данных из всех министерств. В этом контексте обсуждалось возможное незаконное использование баз данных и связанные с этим риски конфиденциальности информации.

В *1970-е гг.* пользование компьютерными системами и данными стало еще более активным. По некоторым оценкам, на конец десятилетия в Соединенных Штатах в эксплуатации находилось около 100 тыс. универсальных ЭВМ. С падением цен компьютерные технологии все более широко применялись в государственном секторе и деловых кругах, а также среди общественности. Это десятилетие характеризуется переходом от доминировавших в 1960-е гг. традиционных имущественных преступлений против компьютерных систем к новым формам преступности. В то время как физическое повреждение оставалось распространенным видом правонарушений против компьютерных систем, появились новые формы компьютерной преступности. Сюда входило незаконное использование компьютерных систем, а также не-

законные манипуляции с электронными данными. В результате перехода от совершаемых вручную операций к использованию компьютеров возникла еще одна новая форма преступности — мошенничество, связанное с применением компьютеров. Уже в то время подобные преступления приводили к многомиллионным убыткам. Мошенничество, связанное с применением компьютеров, являлось настоящей проблемой, и правоохранительные органы расследовали все больше и больше подобных случаев. Поскольку применение существующего законодательства к компьютерным преступлениям вызывало трудности, в различных частях света начались дебаты по поводу возможных юридических решений проблемы. В Соединенных Штатах обсуждался законопроект, разработанный специально для борьбы с киберпреступностью. Интерпол изучал само это явление и возможности для законодательного ответа.

В *1980-е гг.* все более и более популярными становились персональные компьютеры. С появлением этой разработки количество компьютерных систем, а значит, и количество потенциальных целей для преступников снова увеличилось. Впервые среди целей находились самые разнообразные типы критически важной инфраструктуры. Одним из подобных эффектов распространения компьютерных систем был возросший интерес к программному обеспечению, что привело к появлению первых форм программного пиратства и преступлений, связанных с патентами. Взаимозависимость компьютерных систем также стала причиной возникновения новых типов правонарушений. Благодаря сетям, для того чтобы войти в компьютерную систему, правонарушителям необязательно было находиться на месте преступления. Кроме того, получив возможность распространять программное обеспечение через сети, преступники пересылали вредоносные программные средства, и обнаруживалось все больше и больше компьютерных вирусов. Страны начали процесс доработки своих законодательств, с тем чтобы они отвечали меняющимся криминальным реалиям. Международные организации также подключились к этому процессу. Организация экономического сотрудничества и развития (ОЭСР) и Совет Европы создали исследовательские комиссии для изучения явления киберпреступности и оценки возможностей для законодательного ответа.

В *1990-е гг.* введение графического интерфейса (www), за которым последовал стремительный рост числа пользователей Интернета, привело к возникновению новых проблем. Информация, размещенная законным образом в открытом доступе в одной стране, становилась доступной из любой точки мира, т. е. даже в тех странах, где опубликование подобной информации являлось преступлением. Другой связанной с онлайновыми услугами проблемой, которая особенно затрудняла расследование транснациональных преступлений, была скорость обмена данными. Наконец, распространение детской порнографии перешло от физического обмена книгами и видеозаписями к онлайновому распространению через веб-сайты и путем оказания интернет-услуг. В то время как компьютерные преступления носили в целом локальный характер, Интернет превратил электронные преступления в транснациональные. Как результат, международное сообщество стало более активно искать решение проблемы. Резолюция 45/121 Генеральной Ассамблеи ООН, принятая в 1990 г., и выпущенное в 1994 г. Руководство по предупреждению и контролю преступлений, связанных с применением компьютеров, — это лишь два примера предпринятых шагов.

Первое десятилетие нового тысячелетия прошло под знаком новых, крайне изощренных методов совершения преступлений, таких как рассылка подложных электронных сообщений (фишинг) и атаки бот-сети, а также распространение технологий, с которыми правоохранительным органам сложнее работать, таких как передача голоса по IP-протоколу через Интернет (англ. voice over IP, VoIP — голос поверх интернет-протокола) и облачный компьютинг. Изменились не только методы совершения преступлений, но и их масштаб. Поскольку правонарушители получили возможность автоматически совершать атаки, количество правонарушений увеличилось. Страны, а также региональные и международные организации приняли ряд мер, чтобы разрешить усугубляющуюся ситуацию, и сделали борьбу с киберпреступностью своей первоочередной задачей. Новые разработки, такие как большие данные, дроны и носимые технологии, представляют собой области, которые, вероятнее всего, станут объектом внимания правонарушителей в будущем.

§ 3. Современные тенденции киберпреступности

В наиболее полном виде современное состояние мировой киберпреступности выражено в ежегодных докладах Европола «Оценка угроз организованной киберпреступности (IOCTA)».

В докладе 2024 г. Европол сообщает о том, что атаки программ-вымогателей, сексуальная эксплуатация детей и онлайн-мошенничество остаются наиболее опасными проявлениями киберпреступности. Киберпреступный ландшафт оставался разнообразным, включая как

отдельных лиц, так и преступные сети, обладающие широким спектром экспертных знаний и возможностей.

Увеличилось число случаев злоупотребления со стороны киберпреступников легитимными приложениями для обмена сообщениями со сквозным шифрованием (англ. end-to-end encryption, E2EE).

Нормативно-правовая база, направленная на укрепление цифровых систем и повышение безопасности пользовательского опыта, адаптируется, но человеческий фактор по-прежнему остается самым слабым звеном в большинстве сценариев киберзащиты. Многоуровневые модели вымогательства все чаще встречаются во всем спектре киберугроз. Действия правоохранительных органов привели к самороспуску и реорганизации группировок, занимающихся программами-вымогателями, что затрудняет различение брендов программ-вымогателей и злоумышленников, стоящих за этими операциями.

Технологии на основе ИИ делают социальную инженерию еще более эффективной.

Динамика криминального рынка вредоносных программ и фишинговых услуг напоминает динамику законных отраслей, в то время как торговля краденными данными становится главной угрозой, связанной с преступностью как услугой (англ. crime-as-a-servise, CaaS).

Вредоносные большие языковые модели (англ. large language model, LLM) становятся все более заметными инструментами на рынке CaaS. В даркнете уже предлагаются сервисы, помогающие онлайн-мошенникам разрабатывать скрипты и создавать фишинговые письма. LLM также используются в делах о сексуальном вымогательстве, где эти инструменты помогают преступникам усовершенствовать свои методы груминга (в психологии — процесс завоевания доверия ребенка; от англ. grooming — ухаживающий).

Использование дипфейков (от англ. deep learning — глубокое обучение и fake — подделка) — еще одна область, вызывающая беспокойство, поскольку это мощное дополнение к арсеналу киберпреступников. В онлайн-мошенничестве дипфейки используются для имитации голоса, например, для попыток мошенничества с генеральным директором (CEO) и для шоковых звонков, и популярность дипфейков, как ожидается, будет расти. В сфере сексуальной эксплуатации детей (англ. child sexual exploitation, CSE) случаи использования материалов сексуального насилия над детьми (англ. child sexual abuse material, CSAM), созданных с помощью ИИ и модифицированных с его помощью, а также CSAM, полностью созданных с помощью ИИ, уже были

зарегистрированы в 2023—2024 гг. и, как ожидается, станут более заметными в ближайшем будущем.

Криптовалюты. Финансовые преступления, в основном инвестиционное мошенничество и отмывание денег, остаются сферой, в которой криптовалюты встречаются чаще всего. Такие факторы, как рост стоимости некоторых криптовалют и растущее внимание СМИ к криптоинвестициям, также способствуют устойчивому росту случаев инвестиционного мошенничества. В частности, в инвестиционных мошенничествах биткоин все чаще конвертируется в стейблкоины, вероятно, потому что последние менее подвержены волатильности цен.

Некоторые стейблкоины имеют встроенную функцию черного списка в своих смарт-контрактах. Это позволяет правоохранительным органам требовать от компаний заморозки стейблкоинов, которые были идентифицированы как часть кошелька подозреваемого.

Операторы программ-вымогателей чаще всего требуют выкуп в биткоинах, поскольку их все еще проще получить, чем другие виды монет. Однако известны случаи, когда выкуп требовался и в других криптовалютах (например, Monero).

Преступное использование альткоинов (альтернативных криптовалют) растет. Количество дел, поддержанных Европолом, связанных исключительно с биткоинами, практически сравнялось с количеством дел, связанных также с альткоинами. Участие несоответствующих требованиям сервисов остается одной из основных проблем во многих расследованиях, связанных с криптовалютами.

Отмывание криптоденег. Сложность методов обфускации (англ. obfuscate — делать невидимым, запутанным), используемых при отмывании криптовалют, во многом зависит от типа совершенного преступления. В случаях инвестиционного мошенничества, связанного с криптовалютами, часто используются менее сложные методы обфускации, поскольку в большинстве случаев она осуществляется традиционными способами (например, через «денежных мулов», международные банковские счета, перемещение денежных средств и подпольную банковскую деятельность).

Группы в мессенджерах E2EE, похоже, заменили одноранговые платформы для обмена криптовалюты на наличные (а иногда и наоборот, наличных на криптовалюту) и уклонения от проверок на соответствие требованиям.

Подпольные банковские решения и криминальные каналы для отмывания криптовалюты. Активы также, по всей видимости, растут. Возобновилось применение криптовалютных дебетовых карт, которые

можно использовать для быстрого обмена криптовалюты на наличные в банкоматах, отмечен рост использования услуг обмена для отмывания криптовалют.

Обмен в основном производится для обеспечения безопасности и стабильности преступных средств — для безопасности криптовалюты обмениваются на конфиденциальные монеты (например, Monero), для стабильности криптовалюты обмениваются на стейблкоины (например, USDT). В целях соблюдения правил сервисы обмена часто предоставляют правоохранительным органам информацию об источнике, месте конвертации и адресе назначения.

«Темная паутина». Форумы даркнета по-прежнему являются основным каналом рекламы рынков даркнета, хотя некоторые рынки также имеют зеркальные сайты в поверхностном Интернете. Администраторы продолжают ограничивать размер и продолжительность жизни своих рынков, чтобы избежать проверки правоохранительных органов, в то же время пытаясь сохранить большую клиентскую базу, создавая хорошую репутацию через форумы. Среди причин короткой продолжительности жизни рынков даркнета — часто встречающиеся «мошеннические выходы», когда администраторы внезапно закрывают рынок и крадут все средства, хранящиеся на их эскроу-сервисе. Форумы и чаты даркнета по-прежнему являются важной сетевой средой для преступников CSE, чтобы обсуждать CSAM и операционную безопасность (OpSec). Форумы даркнета для преступников CSE все больше специализируются на определенных сексуальных предпочтениях.

Основным бизнесом на рынках даркнета по-прежнему остается *торговля запрещенными наркотическими веществами*.

Программы-вымогатели как услуга. Группы программ-вымогателей, работающие по модели «программы-вымогатели как услуга» (англ. ransomware-as-a-service, RaaS), извлекают выгоду из краха своих конкурентов, чтобы привлечь способных партнеров к своим услугам.

Работа правоохранительных органов против операторов программ-вымогателей наносит ущерб репутации групп в криминальном подполье и оказывает влияние на их партнеров. Блокировка инфраструктуры сервиса программ-вымогателей означает, что партнеры теряют доступ к сервису, где они могут генерировать образцы программ-вымогателей и отслеживать статус своих жертв. Внутренние данные сервиса программ-вымогателей могут содержать персональные данные партнеров и ключи дешифрования для зараженных ими систем. Следовательно, блокировка подвергает партнеров риску быть идентифицированными

и потенциально лишает их рычагов воздействия на жертв. Все это приводит к потере времени, усилий и средств, потраченных на обеспечение первоначального доступа к системам жертв.

Кибератаки становятся все более неконтролируемыми. Эта тенденция может также усугубиться благодаря широкой доступности и повышению качества инструментов ИИ, не обладающих функцией оперативной фильтрации, которые киберпреступники могут использовать для быстрой сборки и отладки своего кода.

Кибератаки преступников, занимающихся вымогательством, в основном нацелены на малый и средний бизнес. Поскольку крупные предприятия могут обеспечить свою кибербезопасность (например, созданием внутренних групп по анализу угроз, повышением устойчивости инфраструктуры и т. д.), простой анализ затрат и выгод позволяет киберпреступникам выбирать организации с менее защищенной инфраструктурой.

Большинство операторов программ-вымогателей выбирают свои цели, основываясь на размере, вероятности выплаты и объеме усилий, необходимых для компрометации систем цели. Это означает, что злоумышленники ищут общедоступные системы и сервисы в инфраструктуре (разведка) и оценивают, какие из них легче всего скомпрометировать.

Первоначальный доступ может быть осуществлен с помощью украденных учетных данных или путем эксплуатации уязвимостей в общедоступных технологиях.

Как и в предыдущие годы, операторы программ-вымогателей продолжают использовать многоуровневые тактики вымогательства. Хотя злоумышленники по-прежнему склонны шифровать взломанные системы, риск публикации или продажи украденных данных на аукционе стал наиболее актуальным фактором давления на жертв, поскольку многие организации начали регулярно создавать резервные копии своих систем.

Сексуальная эксплуатация детей. Внешние факторы, такие как внедрение новых технологий и рост числа детей, находящихся в Сети без присмотра, а также смещение акцентов следственной работы способствовали развитию угроз, исходящих от этой преступной сферы. Сексуальная эксплуатация детей продолжает быть одним из приоритетов для правоохранительных органов, которые имеют дело с постоянно растущим объемом незаконного контента в Интернете.

Материалы о сексуальном насилии над детьми (CSAM) продолжают распространяться в Интернете. В связи с растущим объемом

файлов, подлежащих ручному анализу, и связанной с ними информации о делах правоохранительные органы обнаруживают, что им самим необходима инновационная технологическая поддержка для расследования онлайн-CSAM. Производство и распространение CSAM остается серьезной проблемой, при этом значительная часть обнаруженных материалов теперь идентифицируется как самостоятельно созданные материалы откровенного характера.

Жестокое обращение с детьми на расстоянии (LDCA) представляет собой наблюдение правонарушителей за тем, как один или несколько посредников за плату совершают сексуальное насилие над детьми. Это выделяется как основная форма коммерческой сексуальной эксплуатации детей и как важный источник контента, связанного с использованием видеонаблюдения, которое подразумевает скрытую запись действий жертвы (например, во время видеозвонка или сеанса прямой трансляции).

Транснациональные сексуальные преступники в отношении детей продолжают совершать непосредственные действия против несовершеннолетних, путешествуя и (или) проживая в так называемых странах высокого риска для жертв сексуального насилия. Они действуют на международном уровне, иногда в сотрудничестве с сетью коллег и при поддержке местных посредников. Такие преступники имеют обширные связи и производят значительный объем оригинального контента CSAM, который далее распространяется в интернет-сообществах.

Форумы и чаты по-прежнему остаются важной средой для общения преступников, занимающихся сексуальным насилием, которые обсуждают совершенные преступления в отношении детей и свои фантазии, способы сексуальных домогательств, методы груминга и советы по безопасности. Более опытные преступники обычно общаются на форумах в даркнете, подстраиваются под соответствующие сексуальные предпочтения.

На форумах есть специализированные разделы по техническим вопросам и вопросам безопасности операций (OpSec), где можно найти советы и обучающие материалы. Поскольку эти цифровые среды часто подвергаются удалению с помощью правоохранительных органов, в связи с техническими уязвимостями и DDoS-атаками, срок их существования обычно не превышает двух лет. Чтобы решить эти проблемы, администраторы форумов создают зеркальные сайты, хранящие копию контента, и после закрытия сайта быстро восстанавливают его по новому адресу. Коммуникационные платформы со сквозным шифрованием (E2EE) все чаще используются злоумышленниками для обмена CSAM-материалами и в коммуникационных целях.

Сексуальное вымогательство и жестокий контент в Интернете. Объем самостоятельно созданных сексуальных материалов в настоящее время составляет значительную и растущую долю CSAM, обнаруживаемого в Интернете. Этот контент создается детьми, в первую очередь подростками. Во многих случаях это результат добровольного обмена между сверстниками, но он может быть классифицирован как материал сексуального насилия, как только он был передан третьим лицам без согласия отправителя. Самостоятельно созданные сексуальные материалы также часто являются результатом сексуального онлайн-груминга и вымогательства. В этом случае преступник находит жертву в Интернете, часто на игровых платформах или в социальных сетях, и, войдя в доверие посредством груминга, получает сексуально откровенные материалы и использует их. Они становятся рычагом для вымогательства. Чувство стыда и надежда на прекращение угроз часто побуждают жертв к производству большего количества самостоятельно сгенерированных сексуальных материалов.

Помимо вымогательства нового контента CSAM, некоторые преступники также вымогают у своих жертв деньги. Используя похожий преступный процесс, вымогатели входят в доверие к своим жертвам, выдавая себя за сверстников, ищущих романтических отношений, а затем становятся шантажистами. Они угрожают жертве, что опубликуют в Интернете или разошлют близким знакомым ее откровенное изображение. Жертва часто платит из чувства стыда, и во многих случаях процесс вымогательства длится довольно долго.

Онлайн-группы, распространяющие жестокий и сексуальный контент, часто размещаемые на платформах E2EE, также были признаны рассадниками вымогательства. Эти группы функционируют как культы, где лидеры используют обман и манипуляцию, чтобы сделать своих последователей послушными и зависимыми. Членов подталкивают к распространению экстремальных видео или изображений из-за страха, манипуляций. Получив от жертв персональные данные и откровенные материалы сексуального характера, преступники начинают шантажировать их, заставляя создавать еще более откровенные и (или) экстремальные материалы, направленные на членовредительство, часто в прямом эфире для развлечения других участников группы.

CSAM-контент, созданный искусственным интеллектом. Модели ИИ, способные генерировать или изменять изображения, исполь-

зуются преступниками для создания CSAM-контента и сексуального вымогательства. На выходе получается материал, все больше похожий на настоящий, что затрудняет идентификацию его как искусственно созданного. CSAM, созданные с помощью ИИ, уже были зарегистрированы в 2023 г. и, как ожидается, станут заметны в ближайшем будущем.

Это создает серьезные трудности для правоохранительных органов в выявлении реальных жертв, а также в определении правовых рамок, в которых должно проводиться расследование. Даже в случаях, когда контент полностью искусственный и там не изображена реальная жертва, CSAM-материалы, созданные искусственным интеллектом, все равно способствуют объективации и сексуализации детей. Создание подобных искусственных изображений увеличивает объем CSAM-материалов в обращении и затрудняет идентификацию как жертв, так и преступников. Этот процесс производства также широко доступен и не требует высокой технической квалификации, что потенциально расширяет число и круг преступников. Такие файлы могут легко использоваться для кибербуллинга (от англ. bully — хулиган, грубиян) — травли в Интернете или сексуального вымогательства.

Чем больше объем искусственного CSAM в обращении, тем сложнее будет идентифицировать преступников или жертв с помощью распознавания образов.

Фишинг. Фишинг (от англ. fishing — рыбная ловля) — способ кражи личных данных (пароль, логин и др.) в Интернете — оставался наиболее распространенным видом атак среди схем онлайн-мошенничества (OFS). Смишинг (CMC/текстовый фишинг) был наиболее распространенным видом фишинга, опережая другие разновидности — вишинг (голосовой фишинг) и спуфинг (маскировка под другого человека или компанию). Квишинг, или фишинг с использованием QR-кодов, также появился в 2023 г.

Фишинг как услуга — это быстрорастущий рынок, подобный индустрии. Он предоставляет продукты, услуги и данные жертв, что позволяет все большему числу преступных сетей успешно заниматься фишинговыми атаками, независимо от уровня их организации и технической подготовки.

Зафиксировано даже несколько связанных случаев банковского фишинга, когда аффилированные лица, управляющие различными поддельными интернет-магазинами, параллельно перенаправляли пользователей на поддельные страницы банковских и платежных сервисов. Криптовалюты — наиболее распространенный способ оплаты базовых или премиум-подписок на такие услуги.

Взлом аккаунта. Растущую угрозу представляет *незаконная торговля персональными данными как ключевая форма киберпреступлений как услуги* (CaaS). Захват аккаунтов (англ. account take over, ATO) продолжает иметь целью учетные записи жертв (в онлайн-банкинге, электронной почте или социальных сетях). С помощью ATO преступники также могут похищать средства и получать доступ к цифровым сервисам жертв или конфиденциальной личной информации.

Поскольку банки все чаще рассматривают потерю средств в результате мошенничества с учетными данными как халатность со стороны законного владельца счета, мошеннические схемы, нацеленные на счета физических лиц, остаются для преступников малорискованным и высокодоходным видом деятельности.

Инвестиции, BEC-атаки и романтическое мошенничество. В сфере инвестиций криптовалюты по-прежнему остаются наиболее часто упоминаемым продуктом, предлагаемым жертвам инвестиционного мошенничества. Инструменты удаленного администрирования (RAT) являются незаменимыми для мошенников, осуществляющих подобные операции. Существуют *мошеннические схемы, использующие устройства жертв,* — приложения для криминального инвестирования, доступные для скачивания в легальных магазинах приложений в разных странах и на разных языках. Реклама, генерируемая ИИ, также используется для привлечения потенциальных жертв, и эта тенденция будет нарастать.

Кибератака с использованием деловой переписки (англ. busines email compromise, BEC) остается распространенным видом мошенничества в отношении граждан и частных компаний. В некоторых случаях мошенники используют фишинговые методы для перехвата и манипулирования корпоративной перепиской. Убедительные мошеннические электронные письма можно легко создать с помощью LLM, учитывая постоянный рост и популярность генеративных моделей искусственного интеллекта.

Несмотря на низкий уровень сообщений о романтическом мошенничестве, в основном из-за чувства стыда, испытываемого жертвами, аферы на почве романтических отношений остаются серьезной угрозой. Инструменты ИИ расширяют возможности мошенников не только для того, чтобы охватить большее количество жертв одновременно, но и для того, чтобы усовершенствовать свои методы социальной инженерии.

Скимминг. Цифровой скимминг (от англ. to skim— бегло просматривать, скользить) — мошенничество с банковскими картами — оста-

ется ключевой угрозой, направленной против сайтов интернет-магазинов. Злоумышленники внедряют вредоносный код (также известный как веб-скиммер) на сайты интернет-магазинов, используя различные методы и приемы.

Цифровая скимминговая атака состоит из трех основных частей: загрузчика, вредоносного кода атаки и кражи данных.

Веб-скиммеры могут быть внедрены непосредственно на сервер целевого веб-сайта или путем использования уязвимости в электронной коммерции. Веб-скиммеры также могут быть размещены на сайте с использованием стороннего ресурса, что называется атакой на цепочку поставок. В последнем случае, если страница содержит код с другого домена, злоумышленник может внедрить вредоносный код и обойти большинство мер безопасности. Для передачи украденных данных на C2-сервер злоумышленника используется метод эксфильтрации данных.

Злоупотребление технологиями. Правонарушители все чаще используют распространенные платформы сквозной коммуникации. Более широкое внедрение принципов Web3 (концепция Интернета, основанного на блокчейне) приведет к дальнейшей децентрализации Интернета. В децентрализованном Интернете коммуникации не контролируются и не регулируются ни правительствами, ни частными компаниями. Технология блокчейн и P2P-сети — это два типа децентрализованных коммуникационных сетей, состоящих из частных платформ, полностью контролируемых пользователями. Децентрализация, технология блокчейн и P2P-сети продолжат предоставлять возможности киберпреступникам, поскольку они упрощают анонимное проведение транзакций вне поля зрения властей.

§ 4. Особенности современной киберпреступности в России

Преступления с использованием информационно-телекоммуникационных технологий в 2024 г. составили 40% от общего числа зарегистрированных в России преступлений, что является максимумом от общего числа преступлений с 2020 г. Это следует из материалов МВД России о состоянии преступности.

Всего в 2024 г. в Российской Федерации зарегистрировано 765,4 тыс. киберпреступлений, что на 13,1% больше, чем в 2023 г. «В общем числе зарегистрированных преступлений их удельный вес увеличился с 34,8% в январе — декабре 2023 г. до 40%», — сказано в документах МВД. В 2022 г. IT-преступления составляли 26,5% от общего числа преступлений, в 2021 г. — 25,8%, в 2020 г. — 25%.

По данным МВД России, в 2024 г. четыре преступления из пяти (84,8%) были совершены с использованием Интернета. Всего таких преступлений зарегистрировано 649,1 тыс., это на 23% больше, чем в 2023 г. Также в 2024 г. выросло число киберпреступлений, совершенных с использованием средств мобильной связи. Если в 2023 г. их было зарегистрировано почти 303 тыс., то в 2024 г. это число увеличилось на 14,3% и составило 346 тыс. преступлений.

Финансовый сектор

Финансовый сектор остается в тройке самых атакуемых хакерами отраслей российской экономики. Противостояние кибермошенников, с одной стороны, и банков, регуляторов и вендоров антифрод-решений, с другой, напоминает безостановочную гонку на опережение. При атаках на банки злоумышленники фокусируются на их сотрудниках и контрагентах для проникновения в банковскую инфраструктуру и базы данных. На россиянах — клиентах банков кибермошенники опробуют более продвинутые механики социальной инженерии с использованием возможностей ИИ и новое вредоносное программное обеспечение (ВПО).

По итогам 2024 г. финансовый сектор остался в тройке самых атакуемых хакерами отраслей российской экономики. По данным RED Security, на него пришлось около 17% кибератак — совокупно это более 20 тыс. инцидентов. Чаще всего злоумышленники старались обойти внедренные в банках технические средства защиты от киберугроз, проводили сетевые атаки, а также пытались внедрить ВПО через сотрудников и контрагентов банков, имеющих легальный доступ к инфраструктуре и базам данных кредитных организаций.

Киберпреступников в 2024 г. интересовало не столько непосредственное хищение денег, сколько нарушение стабильности работы ключевых игроков финансовой системы и доступ к большим массивам персональных данных банковских клиентов. По оценке Positive Technologies, именно утечки конфиденциальных данных стали самым частым (71% случаев) последствием атак на финансовые организации.

Злоумышленники уже несколько лет не атакуют финансовые организации с целью получить доступ к их счетам или сети банкоматов. Атаки, связанные с несанкционированным переводом денежных средств, еще случаются, но мошенникам проще добраться до денег через физических лиц. Для этих целей в 2024 г. киберпреступники применяли продвинутые механики социальной инженерии — дипфейковые видеосообщения и сгенерированный медиаконтент в мес-

сенджерах. Число таких дел выросло в 10 раз по сравнению с 2023 г., оценивают в BI.ZONE. Также мошенники не забывали и о проверенных годами методах. Например, в 2024 г. у 90% российских банков в Сети были обнаружены действующие сайты-двойники, которые копировали фирменный стиль бренда. Такие ресурсы позволяли злоумышленникам получать доступ к персональной информации и данным о банковских картах невнимательных пользователей.

Главной проблемой банковских клиентов — физических лиц остается социальная инженерия. Легенды, в которые мошенники будут заставлять верить граждан, эволюционируют. Помимо звонков якобы из «банковских учреждений», «правоохранительных органов», мошенники стали внедрять в скрипты и рутинные ситуации. Сегодня злоумышленники могут не только пугать информацией о якобы возбужденном уголовном деле или попытках вывести деньги со счета, но и использовать в своих схемах обыденные сценарии, например, что нужно забрать обновленный полис ОМС, продлить договор с мобильным оператором. Причем звучат преступники все убедительнее: утечки из медицинских центров, служб доставки и других организаций позволяют собирать объемные профили российских пользователей, отмечают в обзоре киберугроз 2025 г. эксперты ГК «Солар».

Также растет количество атак с использованием сгенерированного искусственным интеллектом контента. Получая доступ к аккаунтам пользователей в мессенджерах, злоумышленники уже научились создавать дипфейки с изображением реальных владельцев взломанных аккаунтов, а их голосовые сообщения и записи телефонных разговоров позволяют получить необходимые фрагменты речи для обучения нейросети.

Киберпреступники продолжают атаковать граждан через ВПО, трояны. Сейчас злоумышленники распространяют их в СМС или мессенджерах под видом ссылок на обновления мобильных приложений «Госуслуги», Минздрава, Минцифры России, ЦБ РФ, а также операторов связи или антивирусов. В 2024 г. появился и Photo Android Malware, который массово распространяется в Telegram под видом фотографий и предназначен для кражи данных и обработки СМС-сообщений, уведомлений, а также выполнения денежных переводов с помощью СМС-сообщений на номер 900. Еще один пример «популярного» сейчас ВПО — технология WebAPK, которая позволяет пользователям устанавливать так называемые прогрессивные веб-приложения на устройства Android без скачивания из Google Play или с сайта компании. Эту технологию киберпреступники используют для кражи данных пользователей через фейковые приложения банков и телеком-операторов.

Наконец, в 2024 г. были зафиксированы первые успешные атаки с использованием программы NFCGate. Это легитимное приложение, предназначенное для захвата, мониторинга и анализа NFC-трафика (англ. near field communication — связь на ближнем расстоянии, NFC) путем его перехвата и воспроизведения. Принцип атаки заключается в перехвате передаваемого NFC-трафика между банковской картой жертвы и NFC-терминалом банкомата, где устройство жертвы считывает NFC-данные банковской карты жертвы, а устройство злоумышленника принимает эти данные и эмулирует их непосредственно рядом с банкоматом, реализуя атаку типа man-in-the-middle.

Киберпреступники продолжат атаковать финансовый сектор через рассылку ВПО на устройства ответственных сотрудников банков. Атаки через подрядчиков банков также являются одним из трендов, так как инструментов и процессов контроля защищенности подрядчиков сейчас де-факто нет, а обнаружить такую атаку достаточно сложно. По данным ГК «Солар», 40—50% инцидентов, которые заканчиваются успешными взломами, проходят по этой схеме.

Тренды киберпреступности

Компания F6, разработчик технологий для борьбы с киберпреступностью, в аналитическом отчете «Киберугрозы в России и СНГ. Аналитика и прогнозы 2024/25» делает выводы: растет число инцидентов и атакующих, количество утечек и атак вымогателей не снижается, DDoS-атаки становятся мощнее, а мошенничество переживает очередной ренессанс.

Как отмечают авторы исследования, в условиях продолжающегося военного конфликта на Украине количество кибератак и число хакерских групп будет и дальше расти. Если в 2023 г. насчитывалось 14 прогосударственных APT-групп, атакующих Россию и СНГ, то в 2024 г. их стало в два раза больше — 27. За 2024 г. было обнаружено 12 новых группировок: Unicorn, Dante, PhantomCore, ReaverBits, Sapphire Cat, Lazy Koala, Obstinate Mogwai, TaxOff и др.

Идеологически мотивированные группы хакеров — хактивисты — продолжают обмениваться опытом и совершенствовать свои навыки и инструменты, что, несомненно, повысит эффективность их атак. В 2024 г. не менее 17 таких группировок атаковали российские и белорусские организации, в 2023 г. их было 13. В своих атаках хактивисты используют различные методы — как DDoS-атаки, так и шифрование, уничтожение данных.

Количество DDoS-атак в 2024 г. выросло минимум на 50%, как и число задействованных в ботнетах (сети из компьютеров, зараженных ВПО) устройств. Наиболее активно атакующей остается группировка IT Army of Ukraine. Аналитики компании прогнозируют: пока продолжается военное противостояние, атаки на российские цели будут идти с нарастающей мощностью.

На этом фоне серьезно трансформируется сам ландшафт киберугроз. Размываются привычные границы классификации преступных групп — хактивистов, прогосударственных APT-групп, киберпреступников. В частности, хактивисты-диверсанты все чаще атакуют государственные органы и компании России, используя в своих атаках программы-шифровальщики — излюбленное оружие финансово-мотивированных злоумышленников. А кибершпионы выкладывают украденные базы данных в публичный доступ в телеграм-каналах, чтобы нанести российским компаниям максимальный урон.

Программы-вымогатели остаются среди главных киберугроз для российских компаний. На протяжении 2024 г. специалисты F6 зафиксировали более 500 атак с использованием шифровальщиков в России — рост почти в полтора раза по сравнению с 2023 г. К уже известным угрозам от вымогателей Shadow, Mimic, LokiLocker/BlackBit, Proxima, HsHarada и др., атакующих российские компании, добавились новые: например, от групп MorLock, Head Mare, Masque, Sauron.

Суммы первоначального выкупа за расшифровку данных в 2024 г. для малого бизнеса составляли от 100 тыс. до 5 млн руб. (1 тыс. долл. — 50 тыс. долл.), а для крупных и средних компаний, на которые приходится каждая пятая атака вымогателей, запросы преступников начинались от 5 млн руб. (50 тыс. долл.). Жертвами вымогателей чаще всего становились российские производственные, строительные, фармацевтические и IT-компании, предприятия добывающей промышленности, ВПК, организации сферы услуг.

Примечательно, что персональные данные остаются одной из главных целей вымогателей: атакующие сначала похищают чувствительную информацию и лишь затем шифруют инфраструктуру жертвы. Чем крупнее цель, тем больше она привлекает злоумышленников: заметен рост количества атак на крупные компании с целью компрометации их клиентов.

Техники и инструменты вымогателей становятся все более сложными и изощренными. В частности, наметился тренд к усложнению атак «персидских групп» (атакующие, предположительно, имеют отношение к странам, где распространен персидский язык), которые

стали все чаще атаковать Linux-системы и использовать для разработки такие современные языки программирования, как Rust.

В целом в 2024 г. было обнаружено 455 не опубликованных ранее баз данных компаний из России и Белоруссии (в 2023 г. их было 246). Количество строк в утечках превысило 457 млн. Дополнительные риски состоят в том, что кроме публикации в открытом доступе злоумышленники используют эти данные для последующего проведения каскадных атак на крупных игроков коммерческого и государственного секторов.

Еще один тренд последнего времени: у русскоязычных преступников исчезает правило «не работаем по Ру» (не атаковать российские организации). В андеграунде можно найти выставленные на продажу базы данных и корпоративные доступы в инфраструктуру компаний из стран СНГ. Так, например, в 2024 г. обнаружена продажа девяти корпоративных доступов стран СНГ. Также было обнаружено сообщение с бесплатной «раздачей» 21 доступа к российским компаниям, одного — к организации из Белоруссии, а еще один доступ из сообщения относился к компании из Украины. Всего же количество «лотов» с предложением доступа в инфраструктуру организаций из стран СНГ в прошлом году выросло на 49% по сравнению с 2023 г. Подобные предложения пользуются повышенным спросом у операторов программ-вымогателей.

Доступ в аккаунты и учетные записи обычных пользователей, данные скомпрометированных банковских карт также являются довольно ходовым товаром у злоумышленников.

Продолжается рост числа фишинговых атак с использованием шпионских программ по модели malware-as-a-service (MaaS). В 2024 г. вредоносные фишинговые рассылки оставались одним из самых популярных векторов проникновения в инфраструктуру цели. В подавляющем большинстве фишинговых писем вредоносное ПО доставлялось во вложениях, которые являются для злоумышленников наименее затратным способом доставки «полезной» нагрузки. Шпионские программы и инфостилеры — самое популярное ВПО в рассылках, в течение 2024 г. их доля варьировалась от 70% до 80% от всех вредоносных семейств, задействованных в фишинговых рассылках.

В ближайшие годы ожидается также увеличение числа атак на цепочки поставок (англ. supply chain attack, SCA) и атак типа Trusted Relationship. В ходе последних хакеры могут получить и использовать легитимные учетные записи для входа в корпоративные сети клиентов поставщиков. В роли поставщиков могут выступать IT-интеграторы, разработчики ПО и другие компании.

Киберпреступники продолжают наращивать объемы фишинговых и скам-атак. Фиксируется рост количества создаваемых ресурсов, эксплуатирующих бренды компаний. В 2024 г. среднее число поддельных ресурсов на один бренд выросло на 28% — с 7878 до 10 112. Среднее количество создаваемых фишинговых сайтов на один бренд увеличилось на 52% по сравнению с 2023 г., мошеннических ресурсов — на 18%. Рост угроз обусловлен продолжающимся развитием мошеннических сообществ и партнерских программ.

С увеличением распространения мобильных устройств на базе Android хакеры продолжают совершенствовать комбинированные методы атак, включая использование фишинга, социальной инженерии и вредоносных приложений. Кроме фишинговых сайтов, похищающих данные банковских карт, злоумышленники активно используют RAT-трояны (трояны удаленного доступа) — их загрузка происходит прямо с фейковых страниц оплаты. Путь к заражению Android-устройств сократился до пары кликов. Начиная с лета 2024 г. злоумышленники распространяли в России и Республике Беларусь троян CraxsRAT под видом легитимных обновлений мобильных приложений «Госуслуги», Минздрава, Минцифры России, ЦБ РФ, операторов связи и антивирусов. Тогда же были зафиксированы первые успешные атаки на клиентов ведущих российских банков с использованием легитимного программного обеспечения NFCGate; злоумышленники предлагают потенциальным жертвам установить на свои Android-устройства приложения на основе NFCGate, и через приложение (NFC-модуль) получают данные банковской карты, которые используют для хищения денег с банковского счета.

За последние годы не только прогосударственные хакерские группировки, но и киберпреступники, а также хактивисты получили доступ к вредоносным киберинструментам, которые могут погрузить мир в цифровые «темные века». Границы между различными типами злоумышленников — хактивистами, государственными хакерами и киберпреступниками — становятся едва различимыми, при этом растет число кибератак и преступных групп. Программы-вымогатели и утечки баз данных будут оставаться в топе главных киберугроз.

Нападения хакеров на российскую промышленность

В 2025 г. число целенаправленных кибератак на российские промышленные предприятия выросло на 20%, отмечают «Информзащита» и Positive Technologies. RED Security выявила в 2025 г. две профессиональные хакерские группы, проводящие целенаправленные

кибератаки на промышленные предприятия. Они применяют специализированные IT-инструменты, ориентированные на конкретных сотрудников или IT-системы компаний. Стоимость таких APT-атак варьируется в зависимости от целей, размера организации и уровня ее защиты, но в среднем их подготовка обходится не менее чем в 1 млн руб.

В тройке наиболее атакуемых отраслей в России — пищевая промышленность (29%), нефтегазовый сектор (23%) и машиностроение (17%). Такое распределение объясняется высокой чувствительностью пищевой отрасли к простоям, стратегической значимостью нефтегазовой промышленности и наличием ценной интеллектуальной собственности в машиностроении.

APT-группировки выявляют уязвимости в IT-системах безопасности предприятий, таких как система планирования ресурсов предприятия (англ. enterprise resource planning, ERP), автоматизированная система управления технологическим процессом (АСУ ТП) и корпоративная почта. Злоумышленники активно используют методы социальной инженерии, вынуждая сотрудников содействовать им через обман, подкуп или шантаж.

Элементы АСУ ТП, в частности системы диспетчерского управления и сбора данных (SCADA), все чаще становятся целями кибератак. Сбой в работе SCADA может привести к остановке производственных линий или полному прекращению работы предприятия, что создает не только экономические и репутационные риски, но и угрозу для жизни людей.

APT-группы избегают прямых кибератак на хорошо защищенные цели. Они ищут уязвимости в цепочке поставок — у подрядчиков, IT-интеграторов или поставщиков программного обеспечения и оборудования с более слабой защитой. Каждая успешная целенаправленная IT-атака может стимулировать APT-группы активнее атаковать объекты критической информационной инфраструктуры (КИИ) в России.

Слабым звеном в кибербезопасности предприятия могут быть бизнес-партнеры и поставщики. Руководители могут сколько угодно усиливать защиту своих IT-систем, но из-за кибератаки на внешнюю компанию хакеры могут получить доступ к данным. Именно supply chain attack остается одной из самых опасных киберугроз с 2019 г. SCA-атака на цепочку снабжения — это кибератака, во время которой хакеры проникают в IT-системы компании через внешнего партнера или поставщика.

Главная угроза SCA-атаки в том, что компании налаживают мощную киберзащиту своих информационных систем, но в то же время им

трудно контролировать всех своих партнеров и подрядчиков, которым они дают доступ к своим данным. Эти предприятия могут иметь более низкий уровень киберграмотности среди сотрудников, более слабые IT-решения по кибербезопасности. Именно этими уязвимостями хакеры и пользуются, атакуя компании-подрядчики и получая доступ к нужным им информационным системам.

В июле — августе 2025 г. пять предприятий российского оборонно-промышленного комплекса (ОПК) стали мишенью кибератак хакерской группировки Cloud Atlas. По данным экспертов Positive Technologies, злоумышленники использовали фишинговые письма с вредоносными документами Microsoft Office, рассылая их на корпоративную электронную почту сотрудников.

Как сообщили в Positive Technologies, открытие зараженного письма могло позволить киберпреступникам проникнуть в инфраструктуру компаний для осуществления кибершпионажа. Тематика вредоносных писем была связана с финансовой, кадровой и мобилизационной деятельностью предприятий. Злоумышленники использовали в качестве приманки приглашения на курсы повышения квалификации, справки о сотрудниках, акты сверки и другие документы, типичные для государственного сектора. Эксперты подчеркнули, что вредоносные файлы представляли собой пустые шаблоны документов, из которых были удалены метаданные для затруднения идентификации источника.

Специалисты Positive Technologies также указали на использование Cloud Atlas характерной техники сокрытия информации об управляющей инфраструктуре. Кроме того, для создания вредоносных файлов хакеры, вероятно, использовали непубличные шаблоны документов Microsoft Office, похищенные из сетей других организаций, ранее подвергшихся атакам.

Мошеннические кол-центры Украины, действующие против россиян

По имеющимся данным, координация мошеннической деятельности против россиян осуществляется с территории Украины. В 2025 г. там действовало от 120 до 150 кол-центров. Широкомасштабная организованная преступная мошенническая деятельность, развязанная украинским режимом на российском направлении, реализуется с задействованием информационной инфраструктуры (энергоресурсы, центры обработки данных, интернет-провайдеры) Украины, а также отдельных стран ЕС. Организаторы находят в России пособников через объявления на специализированных русскоязычных сайтах. Платят пособникам посуточно в криптовалюте, говорится в пресс-релизе ФСБ России от 19 апреля 2025 г.

Завербованным пособникам дают инструкции, предписывающие снимать квартиры на срок до двух недель, причем на верхних этажах таких домов, на первом этаже которых расположены компании, предлагающие услуги автоматизированных телефонных станций. Затем следует приобрести российские сим-карты в большом количестве, зарегистрировать их на подставные данные и разместить на съемной квартире сим-боксы, подключенные к максимально анонимным интернет-провайдерам. Сим-боксы пособники получают из-за границы по почте. После настройки оборудования управление им передается кураторам на Украине.

Кроме того, в некоторых случаях организуются группы пособников, так называемые гастролеры. Они передвигаются между регионами на арендованном автотранспорте, в котором и устанавливают нелегальное оборудование.

Мошенники постоянно совершенствуют механизмы обмана, отметили в ФСБ России. Так, организаторы исключают личное общение с исполнителями или используют их втемную, применяют средства анонимизации — например, позволяющие скрывать и подменять номера телефонов, передавать голосовые и текстовые сообщения в WhatsApp и Telegram, получать подставные платежные реквизиты. Они также прибегают к технологии нейролингвистического программирования, а с помощью ИИ генерируют аудиофайлы и дипфейки.

Атаки на аптечные сети и «Аэрофлот»

В июле 2025 г. российские компании столкнулись с беспрецедентной серией кибератак. Под удар попали как крупнейший авиаперевозчик страны, так и розничные сети. То, что раньше казалось серией разрозненных атак, сегодня начинает обретать очертания единого целого. Этот новый «цифровой фронт» — так можно назвать волну кибердаров по российской инфраструктуре — все чаще рассматривается как инструмент давления и саботажа.

Одним из эпизодов стала атака на аптечные сети «Столички» и «Неофарм» 29 июля 2025 г. В Москве и ряде регионов закрылись десятки аптек, клиенты не могли забронировать лекарства или воспользоваться бонусными картами. На сайтах этих сетей появилось уведомление о технических сбоях, а сотрудники подтвердили, что многие точки временно приостановили работу. По данным телеграм-каналов,

системы аптек были взломаны — на устранение последствий потребовалось не менее суток. Всего аптек «Столички» около 1000, и у «Неофарм» — десятки точек в столице, Петербурге и областях.

28 июля 2025 г. хакеры парализовали информационные системы «Аэрофлота» — крупнейшей авиакомпании России. Утром в этот день компания неожиданно объявила о сбое в IT-системах и была вынуждена отменить 54 рейса (около 42% от всех рейсов дня). В Шереметьево и других аэропортах скопились тысячи пассажиров; за день пострадали не менее 20 тыс. человек. К вечеру того же дня «Аэрофлот» смог частично стабилизировать расписание за счет ручного управления процессами и резервных процедур. Это киберпроисшествие уже назвали одним из самых масштабных в истории гражданской авиации России.

Ответственность за хакерскую атаку взяли на себя две группировки — украинская хактивистская группа Silent Crow и сообщество «Киберпартизаны BY». Злоумышленники заявили, что их операция готовилась в течение года и завершилась успешным проникновением во все ключевые системы авиаперевозчика. По словам хакеров, они сумели получить доступ к компьютерам сотрудников (вплоть до топ-менеджеров), прослушивали переговоры и скопировали 22 ТБ внутренних данных, включая полные базы данных истории перелетов. Атакующие хвастались «уничтожением» около 7000 серверов «Аэрофлота» — от клиентских CRM-систем до почтовых серверов Exchange.

Эксперты отмечают беспрецедентный характер этой атаки. Взломщики не просто вывели из строя сайты, а, судя по их заявлениям, практически «жили» внутри сети «Аэрофлота» многие месяцы. В течение всего предыдущего года были скомпрометированы все критически важные корпоративные системы авиакомпании. Киберпреступники смогли заранее изучить уязвимости, установить свое присутствие и лишь затем нанести решающий удар. Подобный уровень подготовки требует высокой квалификации и значительных ресурсов. Атака явно была целевой: хакеры умело скрывали свое присутствие, возможно, с помощью инсайдерской поддержки и обхода систем мониторинга. По оценкам специалистов, такой взлом — результат длительной разведки, поэтапного проникновения и тщательного сокрытия следов в инфраструктуре жертвы.

Война против нашей страны ведется на всех фронтах, в том числе цифровом. Хактивисты, взявшие на себя ответственность за инцидент, находятся на службе у недружественных государств. Атаку вполне

могли организовать западные спецслужбы или иные профессионалы высокого уровня, использующие хакерские группировки как прикрытие. Действительно, столь длительная и сложная операция, как годичное внедрение в сеть «Аэрофлота», требует немалых ресурсов — человеческих, технических, финансовых. Не исключено, что атаки финансируются из-за рубежа, а непосредственными исполнителями выступают идейные хакеры-активисты. В условиях геополитической конфронтации такая кооперация спецслужб и киберпреступников выглядит вполне реалистично.

Тактика действий преступных групп

Фишинг. Чтобы стало понятно, почему пользователи очень легко попадаются на удочку атакующих и как мошенники обходят меры защиты со стороны банков, следует проанализировать тактику действий преступных групп:

1) атакующие покупают списки уязвимых сайтов самой разной тематики. Таких сайтов на просторах российского Интернета очень много;

2) обладая даже ограниченным доступом к подобному сайту, преступники могут изменять его таким образом, чтобы часть его посетителей перенаправлялась на фишинговую страницу. Если пользователь зашел на «поломанный» сайт в результате поискового запроса в системах Google, Yandex, Bing, Rambler, Mail.ru, его перенаправляют на фишинговый сайт. При этом переход жертвы может быть на любую страницу «поломанного» сайта, кроме главной, иначе перенаправление на фишинговый сайт не осуществляется;

3) фишинговый сайт замаскирован под акцию по розыгрышу призов и информирует жертву о том, что она выиграла денежный приз и может получить деньги. Для этого жертву просят указать данные банковской карты;

4) если жертва указывает данные карты, то на следующем шаге ее просят указать текущий баланс карты;

5) на сайтах разных банков есть услуга перевода с карты на карту. Для того чтобы перевести деньги, необходимо указать данные карты отправителя, получателя, сумму перевода и СМС-код подтверждения. Как только жертва указывает данные о своей карте, программа на сервере хакеров автоматически пытается сделать перевод с карты на карту;

6) жертва должна подтвердить денежный перевод со своей карты с помощью СМС-кода. В этот момент на фишинговом сайте жертве по-

казывают окно, информирующее, что для получения выигрыша нужно ввести СМС-код, полученный на мобильный телефон. Если жертва вводит данный код в поле фишингового сайта, злоумышленники используют его для мошеннического денежного перевода.

Схема очень проста. Она не требует использования вредоносных программ, очень легко масштабируема и позволяет атакующим зарабатывать миллионы рублей. Схема требует, чтобы пользователь указывал все данные сам, но, как показывает исследование, на эти фишинговые страницы попадают тысячи пользователей ежедневно, и среди этих тысяч всегда находятся доверчивые граждане, которые и становятся жертвами мошенников.

Кардинг. Этот сегмент — мошенничество, связанное с незаконным использованием банковских карт без участия владельца — продолжает развиваться очень быстрыми темпами. Сейчас угрозы можно разделить на следующие категории: поддельные POS-терминалы (англ. point of sale — устройство для приема платежных карт), трояны для POS-терминалов и сопутствующие им услуги.

Поддельные POS-терминалы. Злоумышленники осуществляют активный поиск инсайдеров в ритейле, которые готовы подработать за процент. Анализ хакерских форумов показал, что построен целый бизнес по продаже прошивок к POS-терминалам, которые превращают данные устройства в скиммеры. Причем некоторые злоумышленники продают уже прошитые POS-терминалы, другие продают прошивки для них, третьи прошивают POS-терминалы за деньги или процент скомпрометированных дампов (англ. dump — свалка; имеется в виду информация о состоянии компьютерной системы). Когда пользователь расплачивается на кассе, есть риск, что данные его карты в этот момент передаются злоумышленнику.

Трояны для POS-терминалов. Установить поддельные POS-терминалы в точках массовых продаж практически невозможно. Но превратить нормальный терминал в мошеннический можно с помощью специальных вредоносных программ. Одним из первых троянов именно для POS-терминалов был Dexter, о котором сообщили в декабре 2012 г. Можно сказать, что с него и началось широкое распространение данного способа получения дампов карт. Рынок вредоносных программ для POS-терминалов сильно вырос за последнее время. На «черном» рынке продают не только сами вредоносные программы, но и отдельно доступ к терминалам, на которые эти программы можно установить. Программы совершенствуются, появляются новые авторы. Получить доступ к POS-терминалам гораздо проще, чем к процессинговому центру, а вот результат также может быть внушительным. Компрометации POS-терминалов крупных ритейл-сетей позволяют злоумышленникам получать данные миллионов карт.

Сейчас на хакерском рынке большое количество разных программ, которые можно использовать для заражения POS-терминалов, после чего все данные карт, которые будут проходить через терминал, станут известны злоумышленникам. Тактика действий у хакеров следующая:

1) хакеры различными способами находят и заражают POS-терминалы. Для этого они могут использовать вредоносные программы, подбирать пароли к разным серверам, рассылать письма с вредоносными вложениями, использовать инсайдеров в точках, где установлены такие терминалы, и т. п.;

2) после того как вредоносная программа успешно установлена, она начинает собирать из оперативной памяти терминала номера карт и данные магнитной полосы или чипа. Полученные данные отправляются на сервер злоумышленника;

3) собранных данных достаточно для изготовления дубликатов карт, которыми можно воспользоваться при покупке товаров, снятии наличных и т. д.

Хищения через Интернет и мобильный банкинг. Самую большую угрозу для банковских счетов физических лиц представляют банковские трояны для Android-устройств. Более 80% смартфонов в мире работает на платформе Android, не удивительно, что большинство вирусов пишутся именно под нее. Все новые банковские трояны, написанные под Android, умеют похищать деньги автоматически. Они собирают данные банковских карт, и уже не важно, клиентом какого банка является владелец телефона. Зараженный трояном смартфон фактически шпионит за своим владельцем: передает хакерам историю звонков и СМС, доступ к любым файлам на телефоне и информации в облачном хранилище, следит за геолокацией.

Жертва сама загружает и запускает вредоносную программу, иногда следуя инструкциям по установке. Чтобы заставить жертву выполнить эти манипуляции, атакующий распространяет такие программы под видом легальных, например пиратской версии навигатора, средств просмотра фото- или видеофайлов, обновлений операционной системы, расширений и т. п.

С мобильного устройства можно получить абсолютно все данные для совершения мошенничества: данные об остатках на банковском счете; номер банковской карты, срок действия и CVV (Card Validaton Value); СМС-коды для подтверждения платежей; сведения о том, подключен ли

интернет-банк; коды восстановления пароля для доступа в интернет-банк.

Естественно, что злоумышленники начали атаковать именно эти мобильные устройства, получать доступ к описанным выше данным и активно похищать денежные средства.

Одним из наиболее популярных способов хищения является перевод через СМС-банкинг. Пошагово процесс хищения можно представить следующим образом:

1) троянская программа пересылает все СМС на сервер злоумышленника;

2) злоумышленник ищет на сервере СМС с уведомлениями от банков. Например, такие СМС приходят после совершения покупок, и в них содержится информация о балансе банковского счета;

3) если злоумышленник находит номер телефона с интересующим балансом и владелец телефона является клиентом банка, который предоставляет услугу СМС-банкинга, то злоумышленник создает задание вредоносной программе на отправку СМС с информацией о переводе денежных средств на номер банка. При этом все дальнейшие уведомления от банка будут скрываться на телефоне владельца счета и передаваться на сервер злоумышленника;

4) банк отправляет код подтверждения операции на перевод денежных средств по СМС;

5) троянская программа перехватывает СМС от банка, скрывает это сообщение от пользователя и передает его текст на сервер злоумышленника;

6) злоумышленник создает задание вредоносной программе на отправку СМС с кодом подтверждения на номер банка;

7) вредоносная программа выполняет задание, в результате чего операция перевода завершается.

Описанные выше шаги часто автоматизируются, и деньги могут списывать с банковского счета небольшими суммами на протяжении нескольких дней.

Другим популярным способом является сбор данных на мобильном устройстве о банковских картах с последующим переводом с карты на счет хакера. Для сбора данных карт вредоносная программа показывает блокирующее окно, в которое необходимо ввести достоверные данные карты. Такие данные собираются на сервере у хакера, и в нужный ему момент он может начать переводить деньги. Все коды подтверждения платежей будут приходить на тот же номер телефона жертвы и немедленно пересылаться хакеру.

Мошеннические интернет-магазины и сервисы. Это одна из самых простых схем мошенничества. На просторах Интернета существует множество мошеннических ресурсов, где предлагают купить товары по очень привлекательным ценам, но с предварительной оплатой. Многие пользователи идут на риск и в итоге остаются и без товаров, и без денег. Часто отмечаются всплески появления таких мошеннических ресурсов перед большими праздниками.

Кроме мошеннических магазинов есть и *сезонные мошенничества*. Например, перед сезоном отпусков появляются туристические операторы, сервисы по продаже авиабилетов или бронированию отелей. Иногда такие сервисы даже присылают пользователю электронные билеты и квитанции о брони отелей, но они являются поддельными, что выясняется в самый последний момент.

§ 5. Прогноз киберпреступности в мире[1]

Как показывают исследования, страны Европы и Северной Америки входят в число самых безопасных, тогда как страны Латинской Америки и Ближнего Востока подвержены высокому риску киберпреступности. Программы-вымогатели, фишинг и атаки методами социальной инженерии по-прежнему остаются наиболее популярными способами совершения киберпреступлений, в то время как наибольший рост отмечен в сфере криптоджекинга (англ. cryptojacking — теневой майнинг) (136%) и атак на цепочку поставок программного обеспечения (300%).

Страна с наибольшим количеством отклоненных пользователей через процесс KYC (англ. know your customer — знай своего клиента) — США (3,8%), за ней следуют Вьетнам (3,2%) и Индонезия (1,9%). Это также три страны с наибольшим количеством приостановленных или заблокированных аккаунтов из-за потенциально вредоносного использования.

Прогноз стоимости киберпреступности в мире. Киберпреступность продолжает расти, представляя собой одну из самых серьезных угроз глобальной безопасности и экономике. Однако она растет нелинейно — исследование показывает, что она растет экспоненциально.

Используя глобальные данные за период с 2015 по 2024 г. для создания модели прогнозирования, компания Proxyrack прогнозирует,

[1] Прогноз развития мировой киберпреступности дается на основе исследования Международной компании Proxyrack (2 декабря 2024 г.).

что ущерб от киберпреступности во всем мире к 2030 г. составит 19,7 трлн долл. США, что превысит текущий номинальный ВВП Китая.

Экспоненциальный рост стоимости киберпреступности сигнализирует о растущей глобальной угрозе, которая, вероятно, потребует более совершенных стратегий и инвестиций в кибербезопасность. Эта тенденция подчеркивает необходимость разработки профилактических мер и совершенствования системы обнаружения угроз для предотвращения этой эскалации риска.

Киберпреступность по странам. Чтобы оценить риск киберпреступности в разных странах, следует рассмотреть несколько факторов. К ним относятся меры и индексы подверженности киберпреступности, возможности (готовность) к кибербезопасности, цифровое развитие и законодательство.

Четыре страны (Панама, Чили, Коста-Рика, Уругвай), имеют самые большие проблемы с кибербезопасностью. На Ближнем Востоке также, есть некоторые проблемы. Европа лидирует в области кибербезопасности, причем особенно высокие показатели у стран Северной Европы. Франция, Великобритания, Испания и Германия также входят в число стран с самым низким уровнем риска, а США и Канада замыкают список.

Тенденции киберпреступности. Киберпреступность расширилась как по масштабу, так и по сложности, а злоумышленники постоянно совершенствуют свои тактики. Глобальный ландшафт кибербезопасности сталкивается с проблемами программ-вымогателей, фишинга, вредоносного программного обеспечения и криптоджекинга, а также с другими новыми угрозами.

Программы-вымогатели: постоянная угроза. Прогнозируется, что число атак с использованием программ-вымогателей будет расти на 57% в годовом исчислении, а глобальный ущерб к 2031 г. достигнет 265 млрд долл. США в год. Средний размер требуемого выкупа увеличился с 5 млн долл. в 2020 г. до 8 млн долл. США в 2023 г., поскольку злоумышленники используют более агрессивную тактику.

Стали нормой *методы двойного вымогательства*, когда злоумышленники извлекают конфиденциальные данные перед шифрованием систем.

Фишинговые и социальные инженерные атаки. Фишинг составил 36% всех нарушений в мире, 83% организаций сообщили о попытках фишинга.

Рост целевого фишинга, когда злоумышленники нацеливаются на конкретных людей или компании, привел к потерям в размере более 1,8 млрд долл. США, часто используется взлом электронной почты.

Платформы «фишинг как услуга» (англ. phishing-as-a-service, PhaaS) облегчают злоумышленникам запуск крупномасштабных кампаний.

Новые киберугрозы. По мере развития цифрового мира киберпреступники осваивают новые методы атак, используя такие тенденции, как внедрение криптовалюты и облачных технологий.

Криптоджекинг. Криптоджекинг становится предпочтительным методом атаки. CyberScoop сообщает о 136-процентном росте инцидентов криптоджекинга, при этом злоумышленники сосредоточились на высокопроизводительных вычислительных средах.

Количество случаев криптоджекинга, когда хакеры тайно используют вычислительные ресурсы жертвы для майнинга криптовалюты, выросло на 117%. При этом 89,4% вредоносных программ для криптоджекинга были основаны на XMRig — популярном инструменте для майнинга криптовалют.

В настоящее время атаки криптоджекинга все чаще направлены на облачные инфраструктуры из-за недостаточных мер безопасности.

Атаки на цепочки поставок. Dark Reading подчеркивает, что атаки на цепочки поставок выросли на 300% за 2024 г. Злоумышленники используют уязвимости в стороннем программном обеспечении и поставщиках услуг, чтобы проникнуть в высокодоходные цели.

Киберпреступность с использованием искусственного интеллекта. По данным The Hacker News, атаки с использованием ИИ становятся все более изощренными: злоумышленники используют ИИ для автоматизированного фишинга и разработки вредоносного ПО.

Влияние на предприятия и частных лиц. Малые и средние предприятия (МСП) страдают непропорционально сильно: 47% всех кибератак направлены именно на эти предприятия, что приводит к разрушительным финансовым последствиям.

Утечки данных. К 2025 г. общее количество записей, раскрытых в результате утечек данных, превысило 40 млрд, поэтому организациям приходится бороться за защиту личной информации и конфиденциальных данных.

Облачные сервисы все чаще подвергаются атакам: 93% компаний сообщают о проблемах, связанных с вредоносными облачными приложениями и неправильными конфигурациями.

Эти данные подчеркивают значительные финансовые и операционные риски, связанные с киберпреступностью, особенно для МСП, которые чаще становятся объектами атак. Усиление защиты МСП и обеспечение надлежащих облачных конфигураций должны стать приоритетами для снижения потенциальных финансовых потерь и репутационного ущерба.

Инвестиции в кибербезопасность. Несмотря на растущие угрозы, инвестиции в кибербезопасность отстают: только 50% предприятий в США имеют полное киберстрахование.

В Великобритании только 23% предприятий имеют официальную стратегию кибербезопасности. Во всем мире компании, инвестирующие в обучение сотрудников, сообщили о 30-процентном уменьшении количества успешных атак, что свидетельствует о важности образования для защиты от киберугроз. Dark Reading и Krebs on Security выступают за широкое внедрение модели Zero Trust, которая требует проверки каждого пользователя и устройства, независимо от местоположения, для снижения внутренних угроз и латеральных атак.

Передовые технологии, такие как расширенное обнаружение и реагирование (англ. extended detection and response, XDR) и обнаружение угроз на основе ИИ, теперь являются критически важными инвестициями для организаций, стремящихся опережать развивающиеся угрозы.

Киберпреступность и квантовая безопасность. В течение многих лет квантовые компьютеры считались научной фантастикой. Но теперь, когда исследователи быстро продвигаются в их практическом проектировании и внедрении, можно предположить, что эта новая технология сделает традиционную криптографию неэффективной к 2029 г.

Квантовые вычисления манипулируют частицами, используя принципы квантовой механики, расширяя вычисления за пределы традиционных двоичных подходов. Вместо нулей и единиц (или True/False, или On/Off) квантовые компьютеры могут измерять несколько параллельных состояний частицы для хранения информации. Это экспоненциально (на порядки) увеличивает потенциальную вычислительную мощность такого устройства по сравнению с традиционными компьютерами.

Такие возможности имеют огромное значение в ситуациях, где сложность была узким местом, если не прямым препятствием для производительности. Квантовые компьютеры могут решать ранее неразрешимые проблемы и взламывать криптографические шифры, что заняло бы у традиционных компьютеров миллионы лет.

Ключевые игроки в квантовой сфере, такие как IBM, Google и новые стартапы в США и Китае, добились значительного прогресса в масштабировании кубитов, снижении уровня ошибок и создании экосистемы вокруг квантовых технологий.

В 2025 г. квантовые компьютеры еще не стали общедоступными и не способны решать все реальные проблемы. Однако они быстро развиваются в таких нишевых приложениях, как создание лекарств, материаловедение и финансовое моделирование. И многие крупные компании, занимающиеся разработкой вычислительной техники и оборудования, готовятся к квантовому скачку.

Квантовые компьютеры влияют на специфическую нишу — криптографию. Традиционные криптографические системы, такие как RSA и ECC[1], основаны на вычислительной сложности таких задач, как факторизация целых чисел и дискретные логарифмы. Из-за своей ресурсоемкой природы классические компьютеры не могут решать эти задачи.

Однако квантовые компьютеры, работающие на алгоритме Шора, могут решать эти задачи экспоненциально быстрее, потенциально нарушая широко используемые стандарты шифрования.

К достижениям в этих нишевых областях не следует относиться легкомысленно. Так, китайские исследователи взломали 50-битные шифры RSA с помощью квантовых компьютеров. 2025-й — это год, когда эксперты и организации осознали квантовую реальность. Хотя и есть еще некий буфер между настоящим моментом и моментом, когда традиционная криптография станет неэффективной, это лишь вопрос времени.

Таким образом, необходимо начинать думать о постквантовой безопасности. Скорее всего, инициатива будет исходить от регулирующих органов или частных поставщиков услуг безопасности, которые переходят на более продвинутые стандарты постквантовой криптографии.

Квантовое распределение ключей (англ. quantum key distribution, QKD). Эта новая технология, которая использует квантовую механику для защиты коммуникаций, пока еще находится в зачаточном состоянии. Но она обещает дополнительный уровень безопасности для организаций, которые хотят обеспечить будущее своим системам. До-

[1] RSA (англ. Rivest — Shamir — Adleman) — алгоритм шифрования, созданный в 1977 г. Р. Ривестом, А. Шамиром и Л. Адлеманом; ECC (англ. elliptic-curve cryptography) — алгоритм шифрования на основе эллиптических кривых.

полнить ее имеет потенциал постквантовая криптография (англ. post-quantum cryptography, PQC).

Искусственный интеллект. Инструменты на основе ИИ могут помочь в обеспечении квантовой безопасности путем анализа криптографических уязвимостей, рекомендации стратегий внедрения PQC и моделирования квантовых атак для проверки устойчивости системы.

Некоторые из новых стандартов в этой области включают в себя:

— *КРИСТАЛЛЫ-кибер (CRYSTALS-Kyber):* алгоритм на основе решетки, подходящий для механизмов инкапсуляции ключей;

— *Дилитий (CRYSTALS-Dilithium):* схема цифровой подписи, также основанная на решетчатой криптографии;

— *Сфинск+ (SPHINCS+):* схема подписи на основе хеша без сохранения состояния.

Для обеспечения безопасности в квантовую эпоху важна «криптогибкость», когда системы спроектированы так, чтобы быстро переключаться между криптографическими протоколами по мере необходимости. Такая гибкость будет иметь важное значение для поддержания безопасных операций.

Квантовые вычисления оказывают глубокое влияние на рамки соответствия стандартов, регулирующих защиту персональных данных. Существующие стандарты, такие как GDPR, HIPAA и SOC 2, не были разработаны с учетом квантовых угроз. В 2025 г. регулирующие органы и органы по обеспечению соответствия начали осознавать срочность обновления этих программ-фреймворков.

Некоторые грядущие изменения в правилах и системах безопасности:

— *законы о защите данных.* Такие правила, как GDPR, могут потребовать от организаций продемонстрировать квантово-устойчивое шифрование для защиты персональных данных;

— *соблюдение требований финансового сектора.* Учреждения, соответствующие финансовым стандартам (PCI DSS или другим), могут столкнуться с новыми требованиями, квантовой готовности, особенно в отношении безопасности транзакций, для защиты данных в состоянии покоя и в конечном счете в точке продажи;

— *аудит цепочки поставок.* Процессы соответствия стандартам безопасности должны развиваться, чтобы учитывать квантовые уязвимости во взаимосвязанных системах и сторонних поставщиках. Поскольку угрозы цепочек поставок являются одними из самых опасных в современной безопасности, сторонние поставщики являются основными целями для квантовых атак.

Пошаговая дорожная карта для достижения квантовой устойчивости:

— *оценка рисков:* определение системы и приложения, которые полагаются на уязвимые криптографические методы. Приоритетными являются системы, критически важные для непрерывности работы и соответствия;

— *образование рабочей силы:* обучение IT-специалистов и специалистов по безопасности квантовым рискам и стратегиям их смягчения. Директора по информационной безопасности должны взять на себя ведущую роль в обучении членов совета директоров и руководителей по вопросам готовности к квантовым рискам;

— *поэтапная интеграция PQC:* использование гибридного подхода, интегрирующего алгоритмы PQC с существующими криптографическими методами, обеспечение более плавного перехода без ущерба для текущих операций;

— *сотрудничество с органами по стандартизации:* присоединение к глобальным усилиям, таким как инициатива PQC NIST. Сотрудничество помогает организациям опережать появляющиеся стандарты и обеспечивает соответствие передовым практикам;

— *непрерывный мониторинг:* установление надежных структур мониторинга для обнаружения уязвимостей в реальном времени. Квантовая готовность должна быть динамическим процессом, требующим постоянной оценки и обновлений.

Глава 4. Кибертерроризм и киберэкстремизм

§ 1. Истоки использования террористами и экстремистами сети Интернет[1]

Международное джихадистское движение очень рано начало использовать Интернет в своих целях. В 1991 г. был создан сайт Исламского медиацентра (IMC), который, не ограничиваясь пропагандой, давал начинающим боевикам практические советы и рекомендации. Хотя Исламский медиацентр поддерживал джихадистов, он не являлся органом «Аль-Каиды»[2] (англ. al-Qaede, AQ). Только в феврале 2000 г. эта организация обзавелась собственным веб-сайтом (сначала maalemaljihad.com, а с марта 2001 г. — alneada.com). Несколько не-

[1] В данном параграфе использованы материалы исследования М. Экера, доктора политических наук Университета Пантеон-Сорбонна (2015 г.).

[2] Террористическая организация, запрещенная в Российской Федерации.

дель спустя «Аль-Каида»[1] основала свое информационное агентство «Ас-Сахаб», выпускающее различные аудио- и видеоматериалы.

После теракта 11 сентября 2001 г. Соединенные Штаты и их союзники начали операцию «Несокрушимая свобода» (Enduring Freedom). Через несколько недель режим талибов был свергнут, а «Аль-Каида»[1] лишилась базы в Афганистане. Тренировочные лагеря были уничтожены, многие боевики захвачены или убиты. У. бен Ладен и А. аз-Завахири спаслись бегством. Ради выживания «Аль-Каида»[1] была вынуждена менять структуру: на месте централизованной организации с иерархическим устройством возникло множество разрозненных группировок.

Децентрализации ресурсов джихадистов в Сети способствуют и два других фактора.

Во-первых, у крупных сайтов, связанных с «Аль-Каидой»[1], шаткое положение. Они постоянно становятся объектами контртеррористических действий и судебных преследований со стороны правительственных служб или общественных активистов. Так, в 2002 г. сайт alneada.com прекратил деятельность, чтобы позднее открыться под другим именем. Дублирование контента с помощью создания зеркальных ресурсов и частичной передачи данных на сайты сторонников джихадистов рассматривается ими как один из способов укрепить присутствие в Интернете.

Во-вторых, децентрализации способствует эволюция интернет-технологий. Переход от модели Интернета web 1.0 к модели web 2.0 во многом обусловлен развитием технологий, сделавших возможной публикацию контента в режиме онлайн. Ряд пользователей цифровых ресурсов, которые ранее довольствовались лишь чтением веб-сайтов, созданных другими, сами превращаются в создателей веб-контента. Радикальные организации тоже не остались в стороне: джихадизм в его новой версии 2.0 распространяется главным образом через постоянно множащиеся исламистские форумы и социальные сети, где все более заметно присутствие групп, объединенных идеями джихада. К началу 2015 г. около 46 тыс. аккаунтов в Twitter принадлежало членам «Исламского государства» (ИГИЛ)[1] или их сторонникам.

[1] Террористическая организация, запрещенная в Российской Федерации.

§ 2. Пропаганда как главный метод, используемый террористами и экстремистами в Интернете[1]

Одним из основных направлений использования Интернета террористами является пропагандистская деятельность. Обычно пропагандистские материалы имеют форму мультимедийных коммуникаций, содержащих идеологические или практические наставления, разъяснения, оправдания или рекламу террористической деятельности. К ним могут относиться виртуальные сообщения, презентации, журналы, теоретические работы, аудио- и видеофайлы, а также электронные игры, разрабатываемые террористическими организациями или их сторонниками. Тем не менее являющиеся террористической пропагандой материалы, в отличие от законной публичной защиты той или иной точки зрения, нередко носят характер субъективных оценок.

Поощрение насилия является обычной темой пропаганды, связанной с терроризмом. Широкая область влияния распространяемой через Интернет информации в геометрической прогрессии увеличивает аудиторию, на которую она может воздействовать. Кроме того, возможность непосредственного распространения контента через Интернет уменьшает зависимость от традиционных каналов связи, таких как новостные агентства, которые могут предпринять соответствующие шаги в целях самостоятельной оценки достоверности предоставленной информации либо отредактировать и опустить аспекты, считающиеся недопустимо провокационными. Интернет-пропаганда также может включать такой контент, как видеосюжеты о насильственных террористических актах или создаваемые террористическими организациями видеоигры, имитирующие акты терроризма и побуждающие пользователей участвовать в ролевой игре, выступая в роли виртуального террориста.

Пропаганда экстремистской риторики с призывами к насильственным действиям также является общей тенденцией для все более широкого круга интернет-платформ, предоставляющих услуги по размещению информационного наполнения, создаваемого пользователями. Материалы, которые прежде могли распространяться лично или с помощью физических носителей, таких как компакт-диски (CD) и цифровые видеодиски (DVD), среди относительно ограниченной аудитории, все чаще переносятся в Интернет. Такие материалы могут распространяться с использованием широкого спектра инструментальных

[1] В параграфе приводятся положения доклада Управления ООН по наркотикам и преступности «Использование Интернета в террористических целях» (2013 г.).

средств, таких как специализированные веб-сайты, целевые виртуальные чат-группы и чат-форумы, онлайн-журналы, платформы социальных сетей типа X (ранее — Twitter) и Facebook[1], а также популярные видео- и файлообменные веб-сайты типа YouTube и Rapidshare. Использование служб индексации, таких как поисковые системы Интернета, также упрощает процесс нахождения и извлечения информационного наполнения, связанного с терроризмом.

Основная угроза, которую несет с собой террористическая пропаганда, связана с тем, как она используется и в каких целях распространяется. Распространяемая через Интернет террористическая пропаганда охватывает ряд задач и аудиторий. Она может быть приспособлена для воздействия, в частности, на потенциальных или реальных сторонников или противников той или иной организации или общих экстремистских воззрений, на прямых или косвенных жертв террористических актов или на международное сообщество в целом либо какую-то его часть. Ориентированная на потенциальных или реальных сторонников пропаганда может быть направлена на вербовку, радикализацию и подстрекательство к терроризму путем рассылки сообщений с выражением чувств гордости, удовлетворения от успехов и преданности экстремистским целям. Она также может использоваться в качестве доказательства успешного проведения террористических актов для тех, кто обеспечивает соответствующую финансовую поддержку.

Наиболее острую реакцию в мире вызывает стратегия устрашения, практикуемая ИГИЛ[2], и в частности казни граждан западных стран. Запись казней осуществляется профессионально. Члены ИГИЛ[2] взяли на вооружение некоторые приемы из «исламистских снафф-фильмов» (англ. snuff movies — фильмы, в которых показаны реальные пытки или убийства; термин появился в 1970-е гг. в США) А. М. аль-Заркави более чем 10-летней давности. Например, во многих сценах заложники одеты в оранжевую робу, что должно напоминать об узниках американской базы Гуантанамо. Впрочем, между прежними фильмами и материалами ИГИЛ[2] есть существенные отличия. Прежде всего в видеороликах ИГИЛ[2] больше режиссуры: часто применяются спецэффекты, крупные планы и замедленная съемка. Кроме того, видеозаписей казней теперь больше, чем когда-либо раньше. «Исламское государство» разделило свою территорию на несколько административных единиц

[1] Принадлежит компании Meta, признанной экстремистской организацией и запрещенной в Российской Федерации.

[2] Террористическая организация, запрещенная в Российской Федерации.

(вилайетов), каждая из которых распространяет собственные записи с казнями. В результате каждый месяц появляется несколько новых видео с экзекуциями. Среди них сравнительно редко можно видеть казни граждан западных стран, потому что у ИГИЛ[1] не так много заложников с Запада. Зато очень часто показывают расправы над сирийскими солдатами, над «предателями», «коллаборационистами», «шпионами» и «неверными». И, наконец, применяемые ИГИЛ[1] методы устрашения отличаются неслыханной жестокостью. Наряду с обезглавливанием практикуется сжигание заживо, сбрасывание с крыш домов, забивание камнями, утопление, а также использование в качестве палачей несовершеннолетних. Некоторые видеозаписи подобного рода предназначены для западной аудитории, другие — для региональной, третьи — для локальной (сирийских и иракских солдат, преследуемых меньшинств, суннитского населения, вынужденного подчиняться ИГИЛ)[1]. В зависимости об обстоятельств видеозаписи призваны либо внушать людям мысль о необходимости военного вмешательства, либо добиваться подчинения.

«Исламское государство»[1] не пренебрегает идеологической (вернее, политико-религиозной) работой с населением. Ряд пропагандистских видео посвящен открытию религиозных центров, распространяющих исламское учение (дават), или деятельности проповедников, объезжающих подотчетные им округа. Отряды «религиозной полиции» объясняют населению, что дозволено исламскими нормами (в трактовке ИГИЛ[1]), а что запрещено. Некоторые социальные действия, направленные на то, чтобы «завоевать сердца и умы» людей, также снимаются на камеру и выкладываются в Сеть. На других роликах показаны действия ИГИЛ[1] по подрыву враждебных политико-административных структур, такие, например, как убийство политиков или представителей сил правопорядка. Кроме того, ИГИЛ[1] стремится продемонстрировать свою боеспособность и умение вести партизанскую войну. Такие видеоролики часто бывают очень короткими и нечеткими: обычно вылазки боевиков снимают на камеру GoPro. Однако иногда используется гораздо более сложная аппаратура. Некоторые кадры сняты с помощью беспилотников. Часто применяются спецэффекты. Например, в серии видеоматериалов центра «Аль-Фуркан медиа», известной как «Clanging of Swords», а также в 60-минутном «документальном» фильме «Flames of War», выпущенном медиацентром «Аль-Хаят» в сентябре 2014 г., сцены боев сделаны как будто по образцу компьютерных игр типа «Call of Duty», которые пользуются особой популяр-

[1] Террористическая организация, запрещенная в Российской Федерации.

ностью у джихадистов. На некоторых видеороликах запечатлены действия террористов-смертников — таким образом воздается дань уважения «мученикам веры».

Кроме того, пропаганда ИГИЛ[1] направлена на то, чтобы предстать в глазах мировой общественности полноправным государством. Особенно подчеркиваются суверенные права ИГИЛ[1]. Например, право иметь собственную армию: ИГИЛ[1] демонстрирует наличие таких видов оружия, которые может себе позволить только независимое государство. Речь идет об истребителях-бомбардировщиках, ракетных установках. Возможно, ИГИЛ[1] и не умеет обращаться с высокотехнологичным оружием. Однако его наличие должно внушить зрителю образ мощной организации и представление о ее скорой победе в борьбе с правительственными силами. Другой функцией суверенного государства, которую хочет присвоить себе ИГИЛ[1], является правосудие. Джихадисты утверждают, что, требуя строгого соблюдения законов шариата, они, по сути, создают «государство исламского права». Сцены с казнями, с распятием людей, с отрезанием голов воспринимаются в мире как настоящее варварство. Однако для части местного населения казни символизируют определенную форму правосудия. Хотя такое правосудие далеко от западных норм, оно позволяет членам ИГИЛ[1] претендовать на роль восстановителя закона и порядка посреди царящего вокруг хаоса. Известно, например, что, когда иорданский пилот, принимавший участие в бомбардировке Сирии в составе сил международной коалиции, был взят в плен и сожжен заживо, прежде чем расправиться с пленным, представители ИГИЛ[1] консультировались с местным населением относительно методов казни, а в Twitter шло активное обсуждение данного вопроса. Стремясь казаться настоящим государством, ИГИЛ[1] объявило о намерении чеканить собственную монету. В пятом номере англоязычного журнала «Дабик» и первом номере франкоязычного «Дар аль-Салам» представлены изображения новых золотых динаров, прообразом которых послужили монеты, имевшие хождение в VII в., во времена халифа Абд аль-Малика.

Кроме того, ИГИЛ[1] стремится выполнять административные функции. В социальных сетях регулярно появляются фотоснимки официальных документов, которые выпускает «Исламское государство»[1] (удостоверения личности, свидетельства о рождении, дипломы и т. д.). Некоторые видеоролики призваны продемонстрировать заботу о населении подконтрольных территорий: ИГИЛ[1] строит новые дороги, восстанавливает электроснабжение и т. д. Именно этой стороне

[1] Террористическая организация, запрещенная в Российской Федерации.

деятельности ИГИЛ[1] посвящен «документальный фильм», снятый британским журналистом Дж. Кэнтли (который находится у исламистов в заложниках) в Алеппо и распространенный «Аль-Хаятом» в феврале 2015 г. Зрители видят мукомольный завод, узнают о системе исламского образования, внедренной ИГИЛ[1].

В основе подобной пропаганды лежит особая идеология, «джихадистский салафизм». Он представляет собой политико-религиозное учение, которое призывает к неукоснительному следованию шариатским нормам на территориях с мусульманским населением и стиранию установленных западными державами государственных границ ради возрождения исламского халифата. Адепты такой революционной идеологии (конечной целью объявляется свержение существующего порядка и замена его новым, пусть даже новый «порядок» обернется хаосом) считают идеалом ислам VII в., а всю последующую его эволюцию рассматривают как отклонение от истинного пути.

С точки зрения идеологии «Аль-Каида»[1] и ИГИЛ[1] близки друг другу, несмотря на конфликт между их лидерами и кровопролитные столкновения отрядов «Исламского государства»[1] с «Фронтом ан-Нусра»[1]. Игиловцы постоянно ссылаются на У. бен Ладена как на высший авторитет; обе организации ставят целью установление исламского халифата и объединение уммы. Однако их представления о том, когда эти цели могут быть достигнуты, разнятся. Для «Аль-Каиды»[1] провозглашение исламского халифата остается отдаленной перспективой, о которой можно думать только по окончании борьбы, в то время как «Исламское государство»[1] создавало исламский халифат летом 2014 г., стремясь придать джихадистскому движению новое дыхание.

Это событие сопровождалось мощной пропагандистской кампанией по отмене границ, доставшихся в наследство от соглашений Сайкса — Пико[2], и по объединению уммы. Отголоски кампании можно увидеть в видеозаписях казней сирийских солдат, выложенных в Сеть в ноябре 2014 г., где показано, как два десятка игиловцев перерезают жертвам горло. Палачами, совершившими это жуткое деяние, были представители разных стран (в казни участвовали гражданин Франции М. Ошар и британский подданный «Джихади Джон»). Нет сомнений, что целью было продемонстрировать миру, какое влияние имеет ИГИЛ[1] на представителей разных государств.

[1] Террористическая организация, запрещенная в Российской Федерации.

[2] Соглашение от 16 мая 1916 г. между Великобританией, Францией и Российской Империей о разграничении сфер влияния на Ближнем Востоке; согласованный меморандум был подписан британским и французским дипломатами М. Сайксом и Ф. Жорж-Пико.

§ 3. Вербовка, подстрекательство и радикализация новых членов террористических и экстремистских организаций через Интернет

Вербовка. Интернет может использоваться не только в качестве средства для публикации экстремистской риторики и видеоматериалов, но и как способ установления отношений с теми, кто наиболее склонен поддаваться целенаправленной пропаганде, и поиска их поддержки. Террористические организации все чаще используют пропаганду, распространяемую через такие платформы, как защищенные паролем веб-сайты и чат-группы ограниченного доступа в Интернете, в качестве средства тайной вербовки. Совокупная аудитория Интернета обеспечивает террористическим организациям и их сторонникам глобальный резерв потенциальных новобранцев. Интернет-форумы ограниченного доступа становятся для новообращенных тем местом, где они могут узнать о террористических организациях и предложить им свою поддержку, а также приступить к непосредственным действиям, чтобы способствовать террористическим целям. Использование технологических барьеров для доступа к платформам, на которых осуществляется вербовка, кроме того, усложняет процесс отслеживания сотрудниками разведки и правоохранительных органов связанной с терроризмом деятельности.

Террористическая пропаганда нередко специально рассчитана на то, чтобы быть притягательной для уязвимых и маргинализованных групп общества. В процессе вербовки и радикализации террористы, как правило, играют на имеющихся у человека ощущениях несправедливости, изоляции или унижения. Пропаганда может также быть адаптирована таким образом, чтобы учитывать демографические факторы, например возраст или пол, социальные или экономические обстоятельства.

Интернет может служить особенно эффективным средством вербовки несовершеннолетних, которые составляют значительную часть пользователей. Распространяемые через Интернет в целях вербовки несовершеннолетних пропагандистские материалы могут принимать формы мультфильмов, популярных музыкальных видеозаписей или компьютерных игр. Тактика, применяемая на веб-сайтах, которые поддерживаются террористическими организациями или их сообщниками в целях вербовки несовершеннолетних, включает использование смеси мультфильмов и рассказов для детей с сообщениями, в которых поощряются и прославляются террористические акты, такие как миссия террористов-смертников. Аналогичным образом некоторые террористические организации разрабатывают действующие в онлайновом режиме видеоигры, предназначенные для использования в качестве инструментов вербовки и обучения новичков. Такие игры могут служить средством пропаганды применения насилия в отношении государства или видных политических деятелей, предлагая награду за виртуальный успех, и могут выпускаться на разных языках в целях привлечения более широкого круга поклонников.

Подстрекательство. В то время как ведение пропагандистской деятельности само по себе обычно не запрещается, использование пропаганды террористами для подстрекательства к актам терроризма во многих государствах — членах ООН считается противозаконным. В Интернете имеется множество материалов и возможностей для загрузки, редактирования и распространения информационного наполнения, которое может рассматриваться как незаконное превознесение террористических актов или подстрекательство к их совершению.

Важно подчеркнуть различие между простой пропагандой и материалами, имеющими целью подстрекательство к актам терроризма. В ряде государств, для того чтобы привлечь кого-либо к ответственности за подстрекательство к терроризму, требуется доказать наличие необходимого умысла и прямой причинно-следственной связи между предполагаемой пропагандой и реальным заговором или осуществлением террористического акта.

Радикализация. Вербовка, радикализация и подстрекательство к терроризму могут рассматриваться как элементы в цепочке тесно связанных между собой явлений. Радикализация относится прежде всего к процессу идеологической обработки, который нередко сопутствует превращению завербованных неофитов в лиц, преисполненных решимости совершать насильственные действия на основе экстремистских идеологий. Процесс радикализации часто включает использование пропаганды, которая на протяжении длительного времени ведется либо посредством личного общения, либо через Интернет. Продолжительность и эффективность пропаганды и других используемых средств убеждения варьируется в зависимости от конкретных обстоятельств и отношений.

§ 4. Финансирование террористических и экстремистских организаций посредством Интернета

Террористические организации и их сторонники также могут использовать Интернет для финансирования террористических актов. Методы, с помощью которых террористы используют Интернет для мобилизации и сбора средств и ресурсов, можно подразделить на четыре основные категории: прямые просьбы о пожертвованиях; электронная коммерция; использование действующих в Интернете платежных инструментов; посредничество благотворительных организаций.

В случае прямых обращений речь идет об использовании веб-сайтов, чат-групп, массовых рассылок и целенаправленных сообщений в целях передачи просьб о пожертвованиях от сторонников. Веб-сайты также могут использоваться в качестве интернет-магазинов, предлагающих сторонникам книги, аудио- и видеозаписи и другие товары. Платежные средства, предоставляемые в Интернете через специализированные веб-сайты или коммуникационные платформы, позволяют легко осуществлять электронный перевод средств между сторонами. Переводы средств нередко производятся с помощью электронных банковских переводов, кредитных карт или иных платежных средств, доступных через такие сервисы, как PayPal или Skype.

Онлайновые платежные средства также могут использоваться мошенническим путем с помощью таких приемов, как хищение личных данных, кражи кредитных карт, мошенничество с использованием электронных средств коммуникации, биржевое мошенничество, преступления против интеллектуальной собственности и мошенничество на аукционах. Примером использования незаконных доходов для финансирования террористических актов может служить дело «Соединенное Королевство против Юниса Цули». Прибыль от украденных кредитных карт была отмыта несколькими способами, включая перевод через электронную платежную систему e-gold («электронное золото»), которую задействовали для пересылки средств транзитом через ряд стран. Отмытые деньги использовались как для финансирования зарегистрированных 180 веб-сайтов, на которых размещались пропагандистские видеоматериалы движения «Аль-Каида»[1], так и в целях приобретения снаряжения для террористической деятельности в ряде стран. Для незаконного получения примерно 1,6 млн фунтов стерлингов на финансирование террористической деятельности были использованы около 1400 кредитных карт.

[1] Террористическая организация, запрещенная в Российской Федерации.

§ 5. Подготовка террористов и экстремистов в сети Интернет

В последние годы террористические и экстремистские организации все чаще прибегают к использованию Интернета в качестве альтернативной базы для подготовки террористов и экстремистов. Все более широкий спектр средств информации предоставляет платформы для распространения практических руководств в виде интерактивных учебных пособий, аудио- и видеоклипов, информационных сообщений и рекомендаций. На этих интернет-платформах также публикуются подробные инструкции, часто в легкодоступном мультимедийном формате и на нескольких языках, по вопросам о том, например, как вступить в террористические организации, как изготовить взрывчатые боеприпасы, огнестрельное и другие виды оружия или опасные материалы и как планировать и осуществлять террористические акты. Эти платформы выступают в качестве виртуальной учебной базы. Кроме того, они используются, в частности, для обмена специальными методами, приемами или оперативными знаниями в целях совершения террористических актов.

Например, журнал Inspire является интернет-изданием, предположительно выпускаемым «Аль-Каидой»[1] на Аравийском полуострове с заявленной целью дать мусульманам возможность готовиться к участию в джихаде у себя на дому. В нем публикуется большое количество идеологических материалов, направленных на поощрение терроризма, в том числе заявления, приписываемые У. бен Ладену, шейху А. аз-Завахири и другим известным деятелям «Аль-Каиды»[1]. В выпусках журнала публикуются практические учебные материалы о том, как приспособить полноприводный автомобиль для проведения акта нападения на представителей общественности, как боевик-одиночка может осуществить неизбирательное нападение, стреляя из огнестрельного оружия с высокого здания, и т. п.

В имеющихся в Интернете учебных материалах предлагаются инструменты для содействия контрразведывательной деятельности и неавторизованному доступу к компьютерным данным, а также для повышения уровня защищенности противозаконных коммуникаций и деятельности в Сети путем использования доступных средств шифрования и методов анонимизации. Интерактивный характер интернет-платформ помогает создать чувство общности между людьми, живущими в разных географических регионах и имеющими различное

[1] Террористическая организация, запрещенная в Российской Федерации.

происхождение, способствуя созданию сетей для обмена материалами учебного и тактического характера.

§ 6. Планирование террористических операций и экстремистских акций через сеть Интернет

При планировании террористических актов обычно имеет место дистанционный обмен сообщениями между несколькими сторонами.

Через Интернет также могут предприниматься шаги для определения потенциальной цели нападения и наиболее эффективных средств достижения цели террористического акта. Эти подготовительные шаги могут варьироваться от получения инструкций в отношении рекомендуемых методов нападения до сбора информации о предполагаемой цели из открытых и иных источников. Открываемые в Интернете возможности для преодоления расстояний и границ и огромное количество имеющейся в киберпространстве общедоступной информации делают Интернет ключевым инструментом планирования террористических актов.

Секретная связь в процессе подготовки. Самой главной функцией Интернета является обеспечение удобства передачи информации. Террористы становятся все более искушенными в использовании коммуникационных технологий в целях обмена анонимными сообщениями, связанными с планированием террористических актов. В качестве электронного, или виртуального, «тайника» для доставки сообщений террористы могут использовать обычные учетные записи абонентов электронной почты в Интернете. Речь идет о создании черновика сообщения, который остается неотправленным и, соответственно, оставляет минимум электронных следов, но может быть доступен с любого интернет-терминала в любой точке мира для ряда лиц, обладающих соответствующим паролем.

Также существует множество более сложных технологий, которые затрудняют распознавание отправителя, получателя или содержания интернет-сообщений. В Интернете легкодоступны для скачивания средства шифрования и программное обеспечение для анонимизации трафика. Эти инструментальные средства способны, в частности, замаскировать уникальный адрес по протоколу Интернета (IP), идентифицирующий каждое используемое для доступа в Интернет устройство и его местоположение, перенаправить интернет-сообщения через один или несколько серверов в юрисдикции с более низкими уровнями правоприменения в отношении террористической деятельности и (или)

зашифровать данные трафика, относящиеся к посещаемым веб-сайтам. Также может использоваться стеганография[1].

Общедоступная информация. Организации и частные лица нередко публикуют в Интернете значительные объемы информации. В частности, организации размещают рекламу своей деятельности и оптимизируют свое взаимодействие с общественностью. Через поисковые системы в Интернете, способные каталогизировать и извлекать не имеющую надлежащей защиты информацию с миллионов веб-сайтов, можно также получить доступ к некоторому количеству секретной информации, которая может использоваться террористами в противозаконных целях. Кроме того, интерактивный доступ к подробной логистической информации, такой как производимые в режиме реального времени съемки замкнутых телевизионных сетей, а также прикладные программы, например Google Earth, предназначенные для физических лиц и в основном используемые ими в законных целях, могут использоваться в неблаговидных целях теми, кто стремится воспользоваться преимуществами свободного доступа к получаемым с помощью искусственных спутников Земли изображениям, картам и информации о местности и сооружениях в высоком разрешении для ведения рекогносцировки потенциальных целей с удаленных компьютерных терминалов.

В эпоху популярных социальных медиасетей, таких как Facebook[2], Twitter (с 2023 г. — X), YouTube, Flickr и блогерские платформы, частные лица также публикуют в Интернете добровольно или по неосмотрительности беспрецедентное количество конфиденциальной информации. Намерение лиц, распространяющих такие материалы, состоит в том, чтобы донести до своей аудитории новости или иные свежие сведения в информационных или социальных целях. Однако часть этой информации может быть незаконно присвоена и использована в интересах преступной деятельности.

Террористические атаки в Мумбаи в 2008 г., в результате которых погибли 164 человека, показали, что Интернет сыграл важнейшую роль на этапе планирования и во время осуществления этих атак. На этапе планирования террористы провели виртуальную разведку объектов с помощью сетевой картографической службы, что позволило

[1] Стеганография (от греч. στεγανός — скрытый и γράψω — пишу, дословно — тайнопись) — способ передачи/хранения информации при сохранении в тайне самого факта такой передачи/хранения.

[2] Принадлежит компании Meta, признанной экстремистской организацией и запрещенной в Российской Федерации.

им очень точно организовать выполнение задачи, включая определение входов и выходов, которые должны были использоваться на основных объектах атак, и выяснение географических координат объектов, которые были введены в программы устройств GPS.

В процессе самой атаки террористы использовали свои телефоны Blackberry для передачи информации исполнителям, а также для получения инструкций и новой информации от них, например данных о местоположении заложников, о международной реакции на атаки и о действиях полиции. Исполнители использовали каналы VoIP для того, чтобы скрыть свое местоположение. Уровень тактических деталей, о которых становилось известно из социальных сетей, таких как Twitter или Flickr, мгновенно обеспечивал террористам дополнительную ситуационную осведомленность. Опасаясь, что такая информация может помочь террористам, индийские власти даже сами опубликовали твит с просьбой немедленно прекратить публикацию прямых сообщений в Twitter о событиях в Мумбаи.

§ 7. Инструментарий, используемый террористами и экстремистами при совершении преступлений, связанных с Интернетом

Технологический прогресс предоставляет в распоряжение террористов множество современных средств, с помощью которых они могут злонамеренно использовать Интернет в противозаконных целях. Для эффективного расследования деятельности, связанной с использованием Интернета, требуются сочетание традиционных методов ведения следствия, знание доступных инструментальных средств для осуществления незаконной деятельности через Интернет и разработка практических методик в целях выявления, задержания и судебного преследования виновных в совершении таких актов.

Связь на основе интернет-технологий

Протокол передачи голоса через Интернет. За последнее десятилетие выросла популярность приложений, позволяющих пользователям общаться в реальном времени с помощью системы телефонии по протоколу передачи голоса через Интернет (VoIP), видеочата или текстового чата, и они стали более совершенными. В некоторых из этих приложений предусмотрены продвинутые функции по обмену информацией, например позволяющие пользователям совместно работать над файлами или дающие им возможность в реальном времени на удалении наблюдать за экранной деятельностью другого пользователя. Система VoIP, в частности, все чаще используется в качестве эффективного средства общения через Интернет. К числу широко известных провайдеров услуг системы VoIP относятся Skype и Vonage, работа которых основана на преобразовании аналогового звука в сжатый цифровой формат, что позволяет передавать через Интернет пакеты цифровой информации, используя соединения по относительно узкополосным каналам.

Поскольку система телефонии VoIP предполагает передачу пакетов цифровых данных, а не аналоговых сигналов, а провайдеры услуг, как правило, формируют выставляемые абонентам счета за пользование Интернетом исходя из совокупного объема данных, счета за межкомпьютерные вызовы в системе VoIP не выставляются за каждый отдельный вызов, как это делается в традиционных системах мобильной и фиксированной телефонной связи. Такое различие в практике выставления счетов может существенно воздействовать на ход расследований, касающихся обменов сообщениями с использованием системы VoIP, так как при этом правоохранительным органам труднее подтвердить такие обмены маркерами, указывающими, например, на время вызова и местонахождение участников. Однако в качестве средств для установления личности виновных в противозаконной деятельности в Интернете могут также служить другие показатели, такие как время передачи и объем трафика данных в Интернете. Кроме того, в то время как источник и адрес назначения обычных телефонных звонков можно проследить через коммутаторы стационарных линий или антенные мачты сотовой связи, где остаются следы геолокации, обмены сообщениями, осуществляемые с помощью целиком основанной на интернет-технологиях системы VoIP, например через беспроводные сети, могут создавать проблемы для ведущих расследование. Дополнительными осложняющими факторами, связанными с использованием технологии VoIP, могут стать в том числе маршрутизация вызовов через одноранговые сети и шифрование адресов вызова.

Электронная почта. Службы электронной почты на базе интернет-технологий также предоставляют в распоряжение террористов средство скрытого обмена сообщениями, которое может быть злонамеренно использовано в противозаконных целях. Сообщения электронной почты, отправляемые сторонами друг другу, как правило, содержат ряд элементов, которые могут быть полезны для следствия. Типичное письмо электронной почты может состоять из заголовка конверта, заголовка сообщения, тела сообщения и любых связанных с ним

вложений. Хотя в зависимости от настроек применяемого программного обеспечения отображаться может лишь сокращенный вариант заголовка конверта, полный заголовок конверта обычно содержит сведения о каждом почтовом сервере, через который сообщение проходило на пути к конечному адресату, а также информацию об IP-адресе отправителя. Информация, содержащаяся в заголовке конверта, менее подвержена фальсификации (хотя и не застрахована от нее), чем информация в заголовках сообщений, которая обычно состоит из сведений, предоставляемых пользователем, в таких полях, как «Кому», «От кого», «Обратный путь», «Дата» и «Время», фигурирующих на устройстве, с которого отправляется сообщение.

Одним из часто используемых методов для сокращения количества остающихся между сторонами электронных следов и, следовательно, вероятности обнаружения является поддержание связи путем сохранения неотправленных сообщений в папке черновиков учетной записи абонента электронной почты. Тогда эта информация становится доступной ряду лиц, использующих для доступа к этой учетной записи общий пароль. В целях избежания обнаружения могут также приниматься дополнительные меры, такие как использование для доступа к соответствующим проектам сообщений общественных терминалов удаленного доступа, например в интернет-кафе. Данный метод был использован в связи со взрывами бомб террористами в Мадриде в 2004 г.

Кроме того, при передаче сообщений по электронной почте могут использоваться методы анонимизации, например маскирующие IP-адрес, принадлежащий отправителю электронной почты. Могут также использоваться анонимные почтовые серверы, которые удаляют идентифицирующую информацию из заголовка конверта, прежде чем переслать его на последующий почтовый сервер.

Онлайновые службы обмена сообщениями и дискуссионные форумы. Онлайновые службы доставки и отправления сообщений и дискуссионные форумы являются дополнительным средством обмена сообщениями в реальном времени с различной степенью потенциальной анонимности. Онлайновые службы обмена сообщениями обычно позволяют поддерживать двустороннюю связь, тогда как дискуссионные форумы обеспечивают свободное общение между группами лиц. Регистрация в онлайновых службах обмена сообщениями, как правило, осуществляется на основе непроверенной информации, предоставленной пользователем; однако отдельные интернет-службы также фиксируют использовавшиеся при регистрации IP-адреса, которые могут быть затребованы правоохранительными органами на условиях

соблюдения применимых правовых гарантий. Сообщения обычно идентифицируются по уникальному псевдониму, который может назначаться на постоянной основе при регистрации или ограничиваться использованием в ходе конкретного сеанса работы в Интернете. Провайдеры услуг, как правило, не записывают информацию, которой стороны обмениваются во время сеанса работы в онлайновых службах обмена сообщениями, и, следовательно, по завершении сеанса работы в Интернете эта информация может оказаться недоступной для извлечения, а для ее восстановления потребуется прибегнуть к судебной экспертизе жесткого диска одного из участников.

Для того чтобы способствовать развитию чувства общности в мировом масштабе, террористические организации и сочувствующие им могут использовать защищенные паролем дискуссионные форумы. Публикуемые в дискуссионных форумах сообщения могут быть подвержены более тщательному мониторингу и учету со стороны провайдеров услуг, чем двусторонние обмены сообщениями, что повышает потенциальную вероятность получения документальных доказательств в ходе расследований. В ряде юрисдикций сотрудникам правоохранительных органов в связи с проведением расследования разрешается на определенных условиях тайно зарегистрироваться и участвовать под псевдонимом в обсуждениях, которые ведутся в дискуссионных группах.

Файлообменные сети и облачные технологии. Файлообменные сайты, такие как Rapidshare, Dropbox или Fileshare, дают сторонам возможность без труда загружать мультимедийные файлы через Интернет, делиться ими, находить и получать доступ к ним. Методы шифрования и анонимизации, используемые в связи с другими формами интернет-связи, в той же мере применимы к файлам, обмен которыми осуществляется с помощью в том числе пиринговых технологий (P2P) и протокола передачи файлов (FTP). Некоторые файлообменные сети могут вести журналы передачи данных или сохранять информацию о платежах, которые могут представлять интерес в контексте расследования.

Облачные вычисления — это сервис, который предоставляет пользователям удаленный доступ к программам и данным, хранящимся или выполняемым на серверах данных, принадлежащих третьим сторонам. Как и обмен файлами, облачные вычисления представляют собой удобное средство для безопасного хранения, обмена и распространения материалов в Интернете. Использование облачных технологий для доступа к информации, хранимой на удаленных носителях, по-

могает сократить объем данных, хранящихся локально на отдельных устройствах, и, соответственно, уменьшить возможности получения потенциальных доказательств в связи с расследованиями, касающимися использования Интернета в террористических целях.

Серверы данных, используемые для оказания этих услуг, также могут физически находиться в иной юрисдикции, чем зарегистрированный пользователь, с иными уровнями регулирования и возможностями правоприменения. Поэтому для получения ключевых улик в целях проведения судебного разбирательства может быть необходима тесная координация с местными правоохранительными органами.

Методы шифрования данных и сохранения анонимности

Шифрованием данных называется защита цифровой информации от раскрытия путем преобразования ее в криптограмму с использованием математических алгоритмов и ключа шифрования, чтобы она была понятна только намеченному получателю. Средства шифрования могут быть реализованы на аппаратной или программной основе или на основе сочетания того и другого. После шифрования для получения доступа к информации могут потребоваться пароль, фраза-пароль, программный ключ или аппаратное средство доступа либо определенное их сочетание. Шифрование может применяться в отношении данных «в состоянии покоя», содержащихся в памяти таких устройств, как жесткие диски компьютеров, флеш-память и смартфоны, а также в отношении данных «в пути», передаваемых через Интернет, например с помощью VoIP-телефонии и сообщений электронной почты.

К числу примеров распространенных программных средств шифрования можно отнести службы, интегрированные в компьютерные операционные системы или прикладные программы, а также такие автономные программы, как Pretty Good Privacy и WinZip. В рамках дела, слушавшегося в Бразилии, на основе международного сотрудничества и обмена информацией было начато расследование в отношении подозреваемого, которого обвиняли в том, что он участвовал в деятельности джихадистского веб-сайта, связанного с признанной террористической организацией, а именно с «Аль-Каидой»[1], выступал там в качестве модератора и контролировал эту деятельность. На этом веб-сайте размещались видеоматериалы, тексты и обращения боевиков-экстремистов руководящего уровня в переводе на английский язык,

[1] Террористическая организация, запрещенная в Российской Федерации.

чтобы охватить более широкую аудиторию; он также использовался для проведения акций по сбору средств и пропагандистских кампаний расистской направленности.

Полицейская операция, которая привела к задержанию этого подозреваемого, имела целью захватить подозреваемого врасплох, когда он был подключен к Интернету и активно занимался деятельностью, связанной с веб-сайтом. Задержав его в момент, когда его компьютер был включен и соответствующие файлы были открыты, следователи смогли обойтись без симметричных криптографических ключей и других средств шифрования и обеспечения безопасности, использовавшихся подозреваемым и его сообщниками. Таким образом, следователям удалось получить доступ к цифровому контенту, который в противном случае мог бы оказаться недоступным или им было бы труднее овладеть, если бы компьютер был выключен и защищен.

Сокрытие деятельности в Интернете или личности причастных к ней пользователей также может осуществляться с помощью передовых технологий, включая маскирование IP-адреса источника, ложное представление под IP-адресом другой системы или перенаправление интернет-трафика на скрытый IP-адрес. Прокси-серверы позволяют пользователям скрытно выполнять косвенные запросы к другим сетевым службам. Некоторые прокси-серверы позволяют сконфигурировать браузер пользователя таким образом, чтобы трафик браузера автоматически направлялся через прокси-сервер. Прокси-сервер отправляет запросы на сетевые услуги от имени пользователя, а затем задает маршрут доставки результатов снова через прокси-сервер. Использование прокси-серверов может способствовать достижению тех или иных уровней анонимности. Прокси-сервер способен скрыть личность пользователя, выполняя запросы на сетевые услуги без раскрытия IP-адреса, с которого исходит запрос, или намеренно предоставляя искаженный IP-адрес источника. Например, такие прикладные программы, как The Onion Router, могут использоваться в целях защиты анонимности пользователей путем автоматического перенаправления деятельности в Интернете через сеть прокси-серверов, для того чтобы замаскировать ее первоначальный источник. Перенаправление сетевого трафика через несколько прокси-серверов, потенциально находящихся в разных юрисдикциях, повышает степень трудности точного установления отправителя исходящих сообщений.

В качестве альтернативы подозреваемый может взломать IP-адрес законной организации и просматривать информацию в Интернете, используя взломанный адрес. Любые следы такой деятельности были бы

связаны с IP-адресом пострадавшей организации. Через взломанный компьютер подозреваемый также может получать доступ к тем или иным веб-сайтам или хранить на взломанных веб-сайтах вредоносные программы (используемые, например, для получения сведений о кредитных картах или другой личной финансовой информации) в целях избежания опознания.

Существует множество компьютерных программ, которые могут использоваться для сокрытия или шифрования данных, передаваемых через Интернет в противозаконных целях. Эти программы могут включать использование такого программного обеспечения, как «Камуфляж», для маскировки информации с помощью стеганографии или шифрование и парольную защиту файлов с помощью такого программного обеспечения, как WinZip. Может также использоваться многоуровневая защита данных. Например, программа «Камуфляж» позволяет скрывать файлы путем их скремблирования (от англ. scramble — шифровать) и последующего прикрепления в конце файла-носителя по своему выбору. Файл-носитель сохраняет свои первоначальные свойства, но используется в качестве носителя для хранения или передачи скрытого файла. Данное программное обеспечение может применяться к широкому диапазону типов файлов. Скрытый файл, однако, можно обнаружить путем анализа первичных данных файла, который покажет наличие прикрепленного скрытого файла.

Европол в докладах 2015—2025 гг. сообщает о все ширящемся использовании террористами и экстремистами изощренных систем шифрования, включая *шифрованные коммуникаторы*. Террористические и экстремистские группы в настоящее время используют различного рода шифрованные приложения, в основном для коммуникаций, а также для проведения финансовых операций. Существуют также свидетельства, полученные правоохранительными органами стран Южной Азии, что террористы во время атак на объекты городской инфраструктуры активно пользуются шифрованными мессенджерами и шифрованными скайпоподобными платформами.

Известно также, что некоторые террористические группы, принадлежащие к европейской периферии ИГИЛ[1], в P2P-сетях размещали заказы на разработку шифрованных приложений, позволяющих в открытой сети опознавать членов организации, присутствующих в общедоступных социальных сетях.

[1] Террористическая организация, запрещенная в Российской Федерации.

Уязвимым местом террористов является невысокий на сегодняшний день уровень компьютерной грамотности и осведомленности в высоких технологиях. Однако представляется, что данная ситуация в ближайшие два-три года изменится, и террористы, базирующиеся преимущественно в странах Ближнего Востока, откроют для себя мир кибероружия.

Уже сегодня террористы широко используют сеть Tor для монетизации террористических трофеев, рекрутинга и обучения неофитов. Также известно, что более двух третей граждан стран ЕС, отправившихся воевать на Ближний Восток в составе террористических подразделений, как минимум несколько раз посетили рекрутинговые и учебные ресурсы ИГИЛ[1] в сети Tor.

Беспроводные технологии

Беспроводные сетевые технологии позволяют компьютерам и другим устройствам получать доступ в Интернет с помощью радиосигналов, а не через постоянное соединение, например по кабелю. Чтобы получить доступ к сети Wi-Fi, необходимо находиться на относительно небольшом расстоянии от сетевых ресурсов, которое зависит от силы беспроводного сигнала. Беспроводные сети могут быть сконфигурированы таким образом, чтобы позволялся открытый доступ в Интернет без регистрации, или же они могут быть защищены с использованием парольной фразы или различных уровней шифрования. Доступ к беспроводным сетям, зарегистрированным на физических лиц, предприятия или государственные структуры, нередко можно получить из общественных мест. Анонимный доступ к защищенным или незащищенным сетям Wi-Fi может позволять преступникам скрывать связь между их деятельностью в Интернете и идентифицирующей информацией.

Кроме того, в последние годы появился ряд провайдеров услуг, таких как Fon, которые позволяют зарегистрированным пользователям делиться частью пропускной способности своих домашних каналов связи Wi-Fi с другими абонентами в обмен на взаимный доступ к сетям Wi-Fi абонентов по всему миру. В ходе расследования осуществление деятельности в коллективно используемых сетях Wi-Fi существенно затрудняет процесс установления причастности к совершению того или иного деяния единственного правонарушителя, который может быть идентифицирован.

[1] Террористическая организация, запрещенная в Российской Федерации.

Один из нестандартных методов связан с использованием программно определяемых высокочастотных радиоприемников с улучшенными рабочими характеристиками, конфигурируемых через компьютер. Таким образом не происходит обмена данными через сервер и не создается никаких журналов регистрации. Правоохранительным и разведывательным органам сложнее перехватывать сообщения, отправляемые с использованием данного метода, как в плане установления местонахождения передатчиков, так и в плане предсказания в реальном времени частоты, на которой передаются сообщения.

Использование террористами и экстремистами инструментов социальных сетей

Еще в 2011 г. появились сообщения, что 90% террористической и экстремистской деятельности в Интернете осуществляется с помощью инструментов социальных сетей. В настоящее время почти вся их деятельность ведется в условиях относительной открытости социальных сетей. Террористы и экстремисты превратили дешевые и легкодоступные социальные сети в стратегическое средство для коммуникации, поддержания связей, подстрекательств, планирования и т. д. Сами по себе социальные сети потенциально могут действовать как фактор повышения боевой эффективности, увеличивающий организационные способности террористических и экстремистских организаций, их возможности по формированию общественных идей, а также как средство привлечения внимания потенциальных сторонников.

Инструменты сетей, которыми злоупотребляют террористы и экстремисты, включают:

— *тематические чаты*. Они позволяют не только «жителям» Интернета, негосударственным гуманитарным организациям, организациям гражданского общества, но и террористическим группам общаться с единомышленниками и сторонниками по всему миру, вербовать новых последователей и делиться информацией, почти не подвергаясь риску разоблачения властями. Например, среди террористов стал особенно популярен открытый сервис тематических чатов PalTalk, который включает голосовые и видеовозможности. Помимо цели получения поддержки тематические чаты также служат для распространения тактической информации среди «экспертов», поскольку в них даются прямые ответы на такие вопросы, как собрать бомбу или как взломать компьютерную систему;

— *блоги*. В докладе, подготовленном 304-м батальоном военной разведки армии США, подчеркивается, что такие блог-сервисы, как

Twitter (с 2023 г. — X), могут стать для террористов эффективным инструментом координации атак, что было продемонстрировано во время атак 2008 г. в Мумбаи. В отчете также говорится о возможных сценариях использования террористами этого онлайн-формата, включая получение информации о местоположении потенциальных объектов атаки практически в режиме реального времени или, например, взлом страницы солдата и общение с другими солдатами от его имени;

— *сайты социальных сетей*. Виртуальные сообщества становятся все популярнее, особенно среди молодежи. Веб-сайты социальных сетей позволяют террористам обращаться к восприимчивой возрастной группе, которая может сочувствовать их идеям. Кроме того, многие пользователи социальных сетей неосторожно принимают запросы на включение в список «друзей», что может дать террористам возможность получить доступ к их личной информации. Также существуют различные террористические группы, имеющие открытые страницы на сайтах социальных сетей, где любой интересующийся может ознакомиться с размещенной там информацией, почитать дискуссии, посмотреть пропагандистские видеоролики и вступить в такую группу;

— *распространение видеоматериалов*. Террористы используют сетевые платформы, на которых размещаются и распространяются видеоматериалы. Помимо этого, в результате исследования, посвященного высказываниям и комментариям по поводу сетевых видеоматериалов, было установлено, что сетевые видеоматериалы получают глобальную аудиторию, особенно среди молодых зрителей, и такой террористический контент распространяется далеко за пределы своей предполагаемой основной базы поддержки.

Социальные сети, помимо прочего, служат средством распространения практических советов и рекомендаций по использованию всевозможного оружия. Так, существуют сайты, где можно найти подробные инструкции по различным формам ведения вооруженной борьбы.

§ 8. Использование террористами киберпреступности как услуги[1]

Киберпреступность как услуга представляет собой смену парадигмы с точки зрения кибертерроризма. Появление и продолжающийся рост киберпреступности как услуги бросает вызов давно усто-

[1] См.: Доклад Контртеррористического центра ООН при Управлении по борьбе с терроризмом и Межрегионального научно-исследовательского института ООН по вопросам преступности и правосудия (ЮНИКРИ) (апрель 2025 г.).

явшемуся мнению о том, что угроза продвинутых кибертеррористических атак низка, поскольку эти группы и отдельные лица обладают ограниченными возможностями кибератак.

Dark web является важнейшей платформой с точки зрения киберпреступности как услуги и всей экосистемы киберпреступности, выступая в качестве центра для обмена услугами киберпреступности. Однако эта экосистема расширяется, при этом злоумышленники все чаще используют зашифрованные коммуникационные платформы для сбора, общения, продажи незаконно полученных активов и приобретения преступных услуг и продуктов в том, что, возможно, лучше всего назвать криминальным или киберпреступным подпольем.

При попытке подчеркнуть запутанные связи между терроризмом, насильственным экстремизмом и киберпреступностью авторы доклада обнаружили несколько проблем. Главной из них является сложность определения и категоризации этих угроз из-за отсутствия общепринятых определений. На расследование, лежащее в основе этого исследования, также существенно повлияла проблема атрибуции и окончательного понимания личности субъектов угрозы, участвовавших в атаке, и их мотивов. Коллективная природа некоторых групп еще больше усложняет ландшафт угроз, поскольку эти формирования позволяют любому человеку с кибернавыками участвовать в атаках, что затрудняет для правоохранительных органов точную атрибуцию и оценку угроз.

Несмотря на это, собранные доказательства ясно указывают на то, что субъекты угроз, мотивированные системой убеждений, а не чисто финансовыми соображениями, взаимодействуют с киберпреступными элементами в «темной паутине» и более широком киберпреступном подполье в контексте киберпреступности как услуги. Изучение этих субъектов угроз показывает: конвергенция через киберпреступность как услугу может увеличить риск терроризма и кибератак, связанных с насильственным экстремизмом.

Криминальное подполье онлайн-сообществ естественным образом включает в себя «темную паутину» и распространяется по более широкой экосистеме Интернета, включая все более зашифрованные коммуникационные платформы. Явление, известное как «преступление как услуга» — бизнес-модель, в которой преступники предлагают потенциальным клиентам продукты или услуги в обмен на плату, — играет важную роль в этом ландшафте. Эта модель вызывает обеспокоенность, особенно в контексте киберугроз — также известных как «киберпреступность как услуга», — в которых все формы киберпреступности, наряду с другими средствами совершения преступлений, такими как цифровое мошенничество и защищенный хостинг, могут быть приобретены в качестве услуг. Киберпреступность как услуга представляет собой значительный сдвиг парадигмы в мире киберугроз, эффективно «демократизируя» киберпреступность, позволяя лицам с различной степенью технических знаний получать доступ к сложным возможностям и развертывать кибератаки. Более того, эти услуги, управляемые отдельными лицами, работающими в одиночку или группами, структурированными как законные предприятия, нанимающими команды разработчиков, инженеров и представителей технической поддержки, способствуют масштабируемости и коммерциализации киберпреступности в целом, поощряя сотрудничество между киберпреступниками по всему миру и расширяя ее географический охват. Это усилило проблемы, с которыми сталкиваются следователи: отдельные личности скрываются за потенциальными слоями других участников, что делает все более трудным четкое установление атрибуции кибератак, включая понимание мотивов, стоящих за ними.

Терроризм и насильственный экстремизм в киберпреступном подполье. В последние годы террористы идут в ногу с инновациями в использовании Интернета и социальных сетей, в частности, обращаясь к прямой трансляции своих атак в социальных сетях, чтобы усилить свое воздействие. Первый такой случай произошел во время атаки на мечеть в Крайстчерче, Новая Зеландия, в 2019 г., а в 2022 г. — во время атаки на торговый центр Buffalo Mall в Соединенных Штатах Америки.

Хотя эти субъекты продемонстрировали определенную степень мастерства в сфере ИКТ в различных областях, широко сообщается, что им не хватает опыта для осуществления существенных кибератак. Причины их ограниченного участия часто объясняются техническими барьерами для входа в сочетании с отсутствием необходимого финансирования и организационных усилий. Кроме того, существует мнение, что кибератаки не могут обеспечить впечатляющего зрелища физического акта, такого как жестокие атаки, выполняемые даже неформальными или элементарными средствами. Однако зловещий потенциал террористов и их сторонников в плане использования возможностей, представленных в «темной паутине», и извлечения выгоды из киберпреступности как услуги очевиден. Повышенная осведомленность об ИКТ и признаки того, что эти группы осознают альтернативные издержки стратегий кибератак, в сочетании с предположениями о том, что кинетические (или физические) атаки могут стать все более слож-

ными из-за имеющихся контрстратегий, вызывают существенные опасения.

Глобальная оценка угрозы. Выступая на министерских дебатах Совета Безопасности в 2019 г. по вопросу противодействия угрозе терроризма, Генеральный секретарь Организации Объединенных Наций А. Гутерриш привлек внимание к «темной стороне цифрового мира» и «новому рубежу» преступности как услуги. Он отметил тенденции и разработки в социальных сетях и «темной паутине» для координации атак, распространения пропаганды и вербовки новых последователей.

Генеральная Ассамблея также призвала государства-члены работать вместе и с другими соответствующими заинтересованными сторонами, включая академические круги, частный сектор и гражданское общество, для обеспечения того, чтобы террористы не находили убежища в Интернете. При этом она подчеркнула необходимость международного и многостороннего сотрудничества для противодействия тем, кто использует ИКТ в террористических целях, при соблюдении прав человека и основных свобод и соблюдении международного права, а также целей и принципов Устава ООН. Совет по правам человека далее подробно остановился на этих вопросах в последовательных резолюциях о праве на неприкосновенность частной жизни в цифровую эпоху, призвав государства «обеспечить, чтобы любые меры, принимаемые для противодействия терроризму и насильственному экстремизму, способствующему терроризму, которые нарушают право на неприкосновенность частной жизни, соответствовали принципам законности, необходимости и соразмерности и соответствовали их обязательствам по международному праву».

Совет Безопасности ООН также проявлял активность в противодействии использованию ИКТ в террористических целях: за последние годы было принято 15 резолюций, посвященных различным связанным темам, таким как цифровые доказательства, государственно-частное партнерство, краудсорсинг и использование новых методов оплаты. В частности, Совет признал необходимость того, чтобы государства имели возможность проводить расследования в отношении открытого исходного кода и «темной паутины» в контексте борьбы с терроризмом. В октябре 2022 г. Контртеррористический комитет Совета Безопасности принял Делийскую декларацию о противодействии использованию новых и новейших технологий в террористических целях, которая содержит рекомендации по противодействию использованию террористами новых технологий. Декларация является последним признанием Советом Безопасности адаптации террористов к новым и

новейшим технологиям и их использования в террористических целях. В ней также подчеркиваются проблемы, связанные с онлайн-убежищами, и необходимость принятия государствами-членами мер по противодействию использованию новых и новейших ИКТ в террористических целях.

Несмотря на кажущееся признание международным сообществом угрозы и выявленную необходимость сотрудничества и развития потенциала правоохранительных органов и разведывательных служб государств-членов, сохраняется пробел в понимании того, проявилась ли связь между терроризмом и насильственным экстремизмом, а также киберпреступными элементами в темной части Сети в контексте киберпреступности как услуги по проведению кибератак, и если да, то в какой степени.

Шаг в подполье киберпреступности. Важным первым шагом в исследовании киберпреступного подполья является установление четкого понимания отдельных слоев Интернета. Это необходимо для прояснения природы этих слоев, происхождения «темной паутины», ее функционирования и ее роли в киберпреступном подполье.

Слои Интернета. Первый слой Интернета часто называют *«поверхностью», «чистой» или «открытой» сетью,* и это часть, которая индексируется и легко доступна общественности с помощью обычных поисковых систем, таких как Google, Bing или Yandex. Хотя сложно предоставить действительно точные цифры для оценки размера и параметров слоев Интернета, обычно считается, что поверхностная сеть составляет не более нескольких процентов. Одна из оценок в начале 2000-х гг. дала цифру в 5—10%, а сегодня она, вероятно, будет еще меньше, учитывая общий рост Интернета и увеличение неиндексированных данных на оставшихся слоях.

Следующий слой — это то, что называется *«глубокая паутина», или «глубокий интернет».* Это крупнейшая часть Интернета, которая, по оценкам, составляет более 90% от общего объема. Хотя этот термин может заставить некоторых поверить, что это таинственный или, возможно, даже криминальный домен, это не так. Скорее, он относится к части Интернета, которая не индексируется традиционными поисковыми системами, такими как Google, Bing и Yandex, и состоит из контента, для доступа к которому требуются особые учетные данные, разрешения или прямые URL-адреса. Он охватывает широкий спектр контента, такого как защищенные паролем веб-сайты, онлайн-базы данных, частные сети, академические и научные ресурсы, юридические документы и услуги на основе подписки.

Последний слой Интернета — это *даркнет*, также известный как *оверлейные сети*. Доступ к этому слою возможен только через специализированное программное обеспечение, которое обеспечивает повышенный уровень анонимности через одноранговые соединения с использованием нестандартных протоколов и портов. Даркнет управляется функциями анонимности, которые могут обеспечить защиту для лиц, занимающихся незаконной деятельностью.

Распространенные примеры даркнетов: The Onion Router (Tor), The Invisible Internet Project (I2P), Freenet, Zeronet и Lokinet. Однако в Докладе основное внимание уделено Tor, учитывая его широкое признание, большую базу пользователей и историческое значение.

Развитие киберпреступного подполья. Несмотря на историческую и постоянную значимость Tor в формировании даркнета, в последние годы наблюдается заметный сдвиг в его популярности, что требует переосмысления понимания даркнета и существования более широкого киберпреступного подполья при оценке угрозы кибератак со стороны терроризма и насильственного экстремизма.

Растущая культура конфиденциальности привела к всплеску программного обеспечения, ориентированного на конфиденциальность, включая виртуальные частные сети (VPN), ориентированные на конфиденциальность браузеры, операционные системы, которые отдают приоритет анонимности, зашифрованные коммуникационные платформы, провайдеров, предлагающих услуги частной электронной почты, безопасные решения для хранения файлов и децентрализованные сети, а также криптовалюту.

Это распространение дало возможность людям оставаться анонимными, не полагаясь на Tor. Указанные технологии могут предоставлять аналогичную или улучшенную анонимность, делая тех, кто знает, как ими пользоваться, включая потенциально злонамеренных субъектов, менее зависимыми от функций, предоставляемых Tor. В результате незаконная деятельность стала более заметной в более широком цифровом домене за пределами «темной паутины».

Ключевым фактором этого является *растущее использование шифрования* — процесса шифрования данных с целью сделать их доступными только уполномоченным сторонам, включающего преобразование понятного человеку открытого текста в непонятный зашифрованный текст. Использование шифрования привело к появлению различных разработок, в частности *зашифрованных коммуникационных платформ*, многие из которых также широко известны и используются как приложения для обмена сообщениями. Эти платформы используют шифрование для сохранения конфиденциальности сообщений, предотвращая несанкционированный доступ к чатам и звонкам пользователей. Самые безопасные приложения для обмена сообщениями реализуют сквозное шифрование, гарантирующее, что только отправитель и получатель могут иметь доступ к переписке. Использование обмена сообщениями с шифрованием не только защищает данные пользователей, но и повышает общую конфиденциальность. Незашифрованные приложения для обмена сообщениями раскрывают сообщения компании — разработчику приложения, рекламодателям и хакерам. В случае утечки данных личная информация может быть продана в Интернете или использована для кражи личных данных и других киберпреступлений. Таким образом, шифрование имеет решающее значение для защиты целого ряда прав человека, включая право на неприкосновенность частной жизни, свободу мнения и его выражения, а также взаимосвязанные права.

Однако, помимо законного использования, киберпреступники, ищущие инструменты и услуги для сохранения анонимности, используют шифрование для защиты своих коммуникаций и снижения риска утечки информации.

Среди киберпреступников популярными платформами для шифрования коммуникаций являются Telegram, Signal и Discord, причем Telegram был определен как основное средство незаконной киберактивности в 2023 г. Киберпреступники все чаще предпочитают группы Telegram для анонимности и зашифрованного общения службам обмена сообщениями на форумах. В то время как Telegram доминирует с 800 млн пользователей, другие платформы для шифрования коммуникаций не остаются далеко позади. Signal пережил рост загрузок на 677% в январе 2023 г., а Discord с почти 200 млн активных пользователей и полумиллиардом зарегистрированных учетных записей в 2023 г. предоставляет открытую платформу, привлекающую киберпреступников возможностью совершения различных вредоносных действий, таких как фишинг, распространение ВПО и социальная инженерия. В то время как Telegram в основном облегчает преступное общение, функции Discord, как сообщается, использовались злоумышленниками для выполнения различных атак внутри самого приложения. Его возможности обмена файлами, голосовые и видеочаты, а также интеграция с другими приложениями открывают широкое поле для атак злоумышленников. Чаще всего атаки на Discord включают фишинг, где используются подражание и голоса, сгенерированные искусственным интеллектом, а также распространение ВПО через обмен файлами.

Discord имеет много общего с Telegram с точки зрения его использования в преступных целях, включая продажу нелегальных продуктов и услуг, мошенничество.

Рост популярности зашифрованных коммуникационных платформ подчеркивает появление более широкого киберпреступного подполья, при этом «темная паутина» становится всего лишь одним из инструментов в наборе инструментов киберпреступников. Злонамеренные субъекты все чаще отклоняются от эксклюзивного и несколько громоздкого темного веба, исследуют новые пути, такие как зашифрованные коммуникационные платформы, и принимают новые тактики и методологии в соответствии с тем, что предлагают эти пути.

Хотя Доклад фокусируется на «темной паутине» в ее классическом смысле, крайне важно избегать разделения киберпространства — ошибки, которую слишком часто совершают правительства и специалисты по кибербезопасности, — и вместо этого понимать и рассматривать роль «темной паутины» в более широком киберпреступном подполье.

Структуру Интернета можно представить в виде айсберга. «Айсберг Интернета» — это метафора, которая долгое время использовалась для визуального и концептуального объяснения трех его отдельных слоев: поверхностная сеть — видимая часть, глубокая сеть — основная часть подводного мира, а темная сеть — самое основание айсберга. Хотя эта аналогия и полезна для понимания масштаба слоистой природы огромного Интернета, она не может охватить сложность того, что является текучей и развивающейся структурой без статических границ между слоями.

В этом отношении «город Интернета» может быть более подходящим способом концептуализации слоистой и динамической ткани Сети, обеспечивающим более тонкое представление ее разнообразных и взаимосвязанных компонентов. В этой метафоре оживленный центр города с его очень заметной сетью улиц, коммерческих объектов и сияющих башен представляет собой публичные и легко видимые части Интернета, такие как основные веб-сайты и платформы социальных сетей. Внутри этих зданий находятся внутренние механизмы деловой или жилой недвижимости, где люди живут своей личной и частной жизнью, которую представляют собой частные сети и базы данных, составляющие «глубокую паутину». Скрытые углы и темные переулки города, о существовании которых многие жители могут даже не знать, отражают скрытые и иногда опасные уголки «темной паутины». Аналогия с городом охватывает текучесть внутри зданий и между районами, обеспечивая более соотносимое и тонкое представление постоянно развивающейся и взаимосвязанной природы цифрового ландшафта, в котором существует преступное подполье.

Киберпреступность как услуга в киберпреступном подполье. В скрытых закоулках киберпреступного подполья процветает экосистема незаконной деятельности, сосредоточенная вокруг киберпреступных предприятий, которые предлагают киберпреступность как услугу. По оценкам, ежегодный доход от киберпреступности как услуги превышает 1,6 млрд долл. США, киберпреступность как услуга охватывает широкий спектр традиционных видов деятельности, способствующих совершению преступлений, которые легко адаптируются к цифровой сфере. Например, процветают мошеннические сервисы, предоставляющие скомпрометированные кредитные карты для финансирования дальнейших киберпреступных начинаний. Сервисы идентификации предоставляют украденные персональные данные, такие как паспорта, полезные для выдачи себя за другое лицо и обхода проверок «Знай своего клиента» при создании криптовалютных кошельков или обмене фиатной валюты. Обширная экосистема также подпитывает сложные технические элементы киберпреступности, такие как *хакерство по найму для вторжения в сеть, разработка и распространение вредоносного ПО (включая наборы программ-вымогателей), стрессовые инструменты для распределенных атак типа «отказ в обслуживании» (DDoS), возможности социальной инженерии онлайн, фишинговые атаки, эксплойты, подстановка учетных данных и продажа украденных персональных данных.* Концепция киберпреступности как услуги изменила ландшафт этого явления, позволив злоумышленникам получить доступ к различным инструментам, ресурсам и экспертным знаниям, необходимым для выполнения кибератак с повышенной легкостью и эффективностью. Это не только снижает барьеры для входа начинающих преступников, но и облегчает сотрудничество между специализированными лицами или группами, усиливается масштаб и воздействие кибератак при одновременном снижении риска обнаружения.

Приведенные ниже примеры дают лишь беглый взгляд на ландшафт киберпреступности как услуги и предназначены исключительно для иллюстративных целей. Важно подчеркнуть, что киберпреступность — это динамичная и многогранная концепция, которая включает в себя различные типы злоумышленников, каждый из которых вносит свой вклад в постоянно расширяющийся спектр киберугроз. Следовательно, продукты и услуги, доступные для покупки или

аренды в «темной сети», в значительной степени формируются под влиянием меняющихся потребностей и возможностей киберпреступников, достижений в области технологий и последних разработок в области уязвимостей кибербезопасности и мер противодействия. Таким образом, коммерциализация других преступных элементов является очевидной тенденцией, при этом постоянно появляются новые услуги.

Распределенный отказ в обслуживании как услуга (DaaS). DDoS-атака как услуга (DDoS-as-a-Service, DaaS) — это предоставление в аренду имеющихся у злоумышленников возможностей тем, кто хочет запустить распределенные атаки типа «отказ в обслуживании» на свои цели. DDoS-атака происходит, когда злоумышленники заваливают целевой сервер многочисленными запросами, чтобы подавить его и нарушить его способность реагировать на законные запросы. Эта услуга избавляет преступных клиентов от необходимости формировать собственные обширные ботнеты — сети скомпрометированных компьютеров, обычно создаваемые через скомпрометированные устройства Интернета вещей (IoT) — или координировать атаку самостоятельно, атакуя виртуальные частные серверы (VPS) с использованием известных эксплойтов или утекших учетных данных интерфейса прикладного программирования (API).

Наглядной иллюстрацией влияния DDoS-атак является случай с Microsoft. Компания подтвердила, что сбои в работе веб-порталов Azure, Outlook и OneDrive в 2023 г. стали результатом DDoS-атак уровня 7 против ее служб. При DDoS-атаке злоумышленники сосредоточиваются на уровне приложений, перегружая службы огромным объемом запросов, в результате чего службы перестают отвечать, поскольку им трудно обработать огромную нагрузку. Каждый метод DDoS работает, перегружая веб-службу, используя все доступные соединения, делая ее неспособной принимать новые запросы.

Последствия атаки такого масштаба могут потенциально быть многочисленными и неблагоприятными. Хотя Microsoft подтвердила, что не было никаких нарушений данных пользователей после атаки Layer 7 DDoS, такой результат не гарантирован во всех случаях, учитывая потенциальное косвенное воздействие на общую целостность системы. Microsoft признала этот риск и посоветовала пользователям реализовать конкретные меры для усиления защиты от потенциальных последующих атак.

Несмотря на вмешательство правоохранительных органов в последние два десятилетия, DaaS выдержал и продолжает использоваться злоумышленниками с различными мотивами. Развивающаяся тенденция не показывает никаких признаков замедления, при этом компании по кибербезопасности, такие как Cloud-Flare, выявили ошеломляющий рост DDoS-атак — на 532% только во втором квартале 2023 г. Появляются признаки того, что злоумышленники интегрируют DDoS-атаки с другими формами кибератак, такими как программы-вымогатели.

Программа-вымогатель как услуга (RaaS). Эта программа остается широко распространенной киберугрозой с заметными примерами атак на критически важную инфраструктуру, включая поставщиков медицинских услуг и энергии, где злоумышленники стремятся подорвать государственные службы и повлиять на сообщества. Это важное предложение киберпреступности как услуги, которое сыграло ключевую роль в расширении атак программ-вымогателей через партнерские программы. Бизнес-модель вращается вокруг разработчиков программ-вымогателей, создающих и администрирующих онлайн-платформы, которые одобренные партнеры используют для доступа и развертывания программ-вымогателей и обмена извлеченными данными. Взамен разработчики получают процент от платежей программ-вымогателей, сгенерированных партнерскими программами. Эта динамика способствовала распространению групп вымогателей — тенденция, которая, по-видимому, будет продолжаться. При создании партнерских программ разработчики могут отказаться от некоторого контроля над использованием своего ВПО. При этом положения и условия будут согласованы с партнерами, чтобы включить ограничения на использование, например соглашения не нацеливаться на определенные типы учреждений. Это обычная практика в «темной паутине». Однако соблюдение этих ограничений не всегда гарантировано. Кроме того, способность разработчиков и аффилированных лиц отмежеваться друг от друга добавляет уровень сложности к атрибуции, создавая дополнительные проблемы для расследований правоохранительных органов.

Весьма показательной иллюстрацией далеко идущих последствий атак программ-вымогателей является инцидент 2021 г. с участием Colonial Pipeline. Эта кибератака вывела из строя трубопровод, вызвав массовую панику в Соединенных Штатах и привлекая внимание всего мира. Атака привела к остановке работы Colonial Pipeline примерно на пять дней, что стало причиной локального дефицита бензина, дизельного топлива и авиатоплива и вызвало панические закупки из-за неизбежного истощения запасов газа. Атака также имела более широкие социальные и финансовые последствия, побудив Colonial Pipeline заблаговременно отключить свои операционные технологические си-

стемы, чтобы предотвратить дальнейшее заражение. В итоге компания заплатила хакерам 4,4 млн долл. США в криптовалюте для восстановления своих операционных систем. Несмотря на получение ключа дешифрования, на перезапуск трубопровода потребовалось несколько дней.

Доступ как услуга (AaaS). Это растущее расширение модели киберпреступности как услуги, где злоумышленники предлагают точку доступа к деловым сетям в качестве продукта (англ. access-as-a-service, AaaS). Преступники, известные как брокеры первоначального доступа (англ. initial access brokers, IAB), продают доступ к компрометированным корпоративным сетям. Они действуют либо как продавцы, управляя своими предприятиями с помощью структурированных маркетинговых стратегий и интернет-магазинов поставщиков (эта услуга не включает предоставление непрерывного доступа, она представляет собой продукт, обычно состоящий из набора учетных данных вместе с VPN-сервером для подключения), либо как посредники (эта функция может привести к неблагоприятным последствиям в различных секторах и служит ценным инструментом для злоумышленников, желающих выполнить последующие кибератаки, независимо от их основных мотивов).

Рост AaaS усилил угрозу атак программ-вымогателей с 2020 г. Хотя программы-вымогатели явно доминируют в воздействии таких нарушений, молчаливые посредники — те, кто скрытно продает доступ другим злоумышленникам, — играют решающую роль в обеспечении этих атак. Эта динамика подразумевает положительную корреляцию: предполагается, что по мере того, как атаки RaaS и программ-вымогателей продолжат расти, AaaS, вероятно, последует их примеру.

Украденные данные как услуга (SDaaS). Общей нитью, связывающей вышеупомянутые вредоносные действия, является приобретение и эксплуатация украденных данных, которые служат ценным незаконным товаром, представляющим собой виртуальную золотую жилу для дальнейших потенциальных угроз. В результате украденные данные как услуга (англ. stolen data-as-a-service, SDaaS) возникают как побочный продукт кибератак и ключевой фактор для последующих вредоносных действий. Регулярно обмениваемые в киберпреступном подполье, украденные данные становятся высокодоходным и востребованным продуктом, от которого должны защитить меры кибербезопасности.

Несколько примечательных примеров крупнейших утечек данных в истории включают Yahoo (2013 г.) с 3 млрд записей, First American Corporation (2019 г.) с 885 млн записей и Indian Council for Medical

Research (2023 г.) с 815 млн записей. По оценкам, в 2023 г. во всем мире было украдено ошеломляющее количество записей — 8 214 886 660, и ожидается, что эта цифра будет увеличиваться в сочетании с общим прогнозируемым ростом киберпреступности. Эти атаки могут привести к различным социальным и финансовым последствиям, а утечка конфиденциальной правительственной информации может иметь политические, финансовые и связанные с конфиденциальностью последствия. Продажа данных в «темной паутине» не только приносит доход, но и усиливает воздействие атаки, передавая конфиденциальную информацию в руки других злоумышленников.

Для компаний, занимающихся кибербезопасностью, SDaaS — серьезный вызов. Это высокодоходный бизнес, 93% поставщиков которого в первую очередь руководствуются финансовыми мотивами. Учитывая финансовую выгоду, SDaaS будет оставаться значительной угрозой для кибербезопасности.

Терроризм, насильственный экстремизм и киберпреступность как услуга в «темной паутине». Стремление террористических групп и отдельных лиц разрабатывать киберстратегии очевидно, поскольку участие определенных террористических групп в кибератаках было замечено еще во времена «Аль-Каиды»[1] в конце 1990-х гг. Примечательно, что в 2011 г. группа выпустила широко освещаемое видео, в котором объявила «электронный джихад» против Соединенных Штатов Америки и призвала своих последователей начать кибератаки на критически важную инфраструктуру США. «Исламское государство»[1] отразило эти стремления в различных призывах на протяжении всего своего подъема к известности, побуждая сторонников взламывать вебсайты западных правительств. В декабре 2023 г. террористы выступили с конкретным призывом к атакам на сайты, связанные с еврейской общиной, через публикацию в темной сети «Голос Хоросана». «Хакерское подразделение Исламского государства», «Кибермармия Халифата» и «Объединенный киберхалифат» — хакерские группы, связанные с ИГИЛ1, — находились на переднем крае киберактивности группировки и сыграли ключевую роль в широком использовании ею социальных сетей.

Нельзя игнорировать угрозу значительных кибератак со стороны террористических группировок в будущем. Например, ИГИЛ[1] активно стремился вербовать в свои ряды лиц, обладающих навыками кибератак, и были зарегистрированы случаи, когда при отсутствии внутрен-

[1] Террористическая организация, запрещенная в Российской Федерации.

них знаний террористические группы и отдельные лица пытались использовать знания завербованных.

Это было наиболее заметно в случае с А. Феризи, или «Th3Dir3ctorY», — хакером, который в 2015 г. получил доступ на уровне системного администратора к серверам в Соединенных Штатах Америки и извлек личную информацию приблизительно 1300 военнослужащих и государственных служащих США. Впоследствии он связался с членами ИГИЛ[1] через Twitter и Skype и передал эту информацию «Хакерскому отделу Исламского государства», который впоследствии опубликовал данные.

За последнее десятилетие террористические группы продемонстрировали все более высокую техническую осведомленность. Некоторые могут похвастаться специализированными техническими группами, которые разрабатывают и пропагандируют инновационные методы уклонения от правоохранительных органов. Это согласуется с расширенным использованием «темной паутины» и технологий в киберпреступном подполье. Например, ИГИЛ[1] и «Аль-Каида»[1] приняли Rocketchat, децентрализованное программное обеспечение с открытым исходным кодом, которое позволяет пользователям устанавливать свои собственные серверные экземпляры. Этот стратегический шаг позволил этим группам создать еще более безопасные и приватные каналы связи. Их изощренность также распространяется на дополнительные возможности уклонения, предназначенные для того, чтобы помешать службам безопасности. Например, в 2022 г. поддерживающая возможности кибербезопасности ИГИЛ[1] «Electronic Horizon Foundation» опубликовала короткое обучающее видео на своем темном веб-сайте и в социальных сетях о программе «Locker», которая автоматически стирает все данные после нескольких неудачных попыток разблокировать устройство. Они также продемонстрировали возросшее понимание технологии блокчейн и криптовалюты, которые широко представлены в качестве услуг в «темной паутине». Биткоин был первой криптовалютой, которую эти группы использовали для кампаний по краудфандингу, и он остается обычным явлением в деле широкого финансирования терроризма и отмывания денег. Недавние тенденции также указывают на сдвиг в сторону менее восприимчивых к отслеживанию криптовалют, таких как Monero, более ориентированный на конфиденциальность, который в основном используется для кампаний по сбору пожертвований, децентрализованных финансов (DeFi), смешанных сервисов и перекрестного подключения к альтернативным блокчейнам, при этом широко используются стейблкоины TRON и Tether (USDT).

[1] Террористическая организация, запрещенная в Российской Федерации.

Также имеются некоторые свидетельства кибервозможностей и намерений определенных лиц, вдохновленных терроризмом на основе ксенофобии, расизма и других форм нетерпимости или во имя религии либо убеждений (XRIRB).

Так, хакер, предположительно мотивированный теориями заговора вокруг COVID-19, распространил около 25 тыс. учетных записей электронной почты от Фонда Гейтса, Всемирной организации здравоохранения и Центра США по контролю и профилактике заболеваний на неонацистском канале Telegram.

В последние годы также наблюдается заметный рост киберпреступности со стороны злоумышленников, предположительно мотивированных и другими соображениями, отличными от финансовых. Таких лиц и группы, или «коллективы», часто называют хактивистами, и они стремятся использовать кибератаки для продвижения своих политических, религиозных или социальных убеждений, нацеливаясь на организации, воспринимаемые как противники или связанные с противоположными системами убеждений. Технические возможности этих злоумышленников могут различаться, но их текучесть позволяет призывать к действию киберпреступников с любым набором кибернавыков в поддержку различных целей. Яркими примерами таких групп являются Anonymous — децентрализованный коллектив хактивистов, — а также GhostSec, ThreatSec, SiegedSec, Killnet и AnonymousSudan, и это лишь некоторые из них. Примечательно, что эти группы заявляют, что нацелились на критически важную инфраструктуру, включая больницы и коммунальные системы, и выражают явное намерение максимизировать общественное воздействие, нанося значительный ущерб, с явным пренебрежением к вреду невинным людям.

Некоторые из этих групп пытаются дистанцироваться от такого изначально очевидного пренебрежения к вреду для населения. В октябре 2023 г. Международный комитет Красного Креста выпустил набор руководящих принципов, в котором изложены правила ведения боевых действий для гражданских хакеров, участвующих в конфликте, основанные на международном гуманитарном праве, что было одобрено некоторыми группами хактивистов, в частности Killnet, который обязался соблюдать руководство. Однако, несмотря на такие события, это общее явление в ландшафте субъектов угроз имеет большое значение в свете растущих масштабов кибератак и размывает попытки разли-

чить действия, совершаемые преступниками или экстремистами, по их природе.

Важно подчеркнуть, что преступность, хактивизм, терроризм и насильственный экстремизм не следует смешивать, тем более в отсутствие согласованных на международном уровне определений и с учетом опасений, что определения во многих национальных юрисдикциях либо отсутствуют, либо недостаточно ясны и точны, чтобы соответствовать международному праву в области прав человека, включая гарантию права на свободу выражения мнения. В то же время должны быть эффективными и соразмерными меры, принимаемые правоохранительными органами и уголовным правосудием, чтобы привлечь преступников к ответственности за кибератаки, защитить права жертв и предотвратить дальнейшие атаки.

Торговые площадки dark web. Торговые площадки даркнета — это коммерческие веб-сайты, доступ к которым осуществляется через зашифрованный браузер, которые функционируют в основном как черные рынки для незаконной торговли. Несколько источников подчеркнули связь между субъектами угроз и торговыми площадками даркнета. Были замечены связи с терроризмом. Например, оружие, использованное при атаках в Париже, Франция, в 2015 г. и в Мюнхене, Германия, в 2016 г., предположительно было приобретено у поставщиков, работающих в даркнете. Также широко сообщается, что средства мошенничества, такие как украденные кредитные карты и паспорта, были приобретены террористическими группами на торговых площадках даркнета. Хотя это подтверждает четкое указание на то, что торговые площадки даркнета используются террористическими группами и отдельными лицами, недостаточно информации, чтобы установить истинную природу взаимодействий и определить, в какой степени их можно отнести к кибератакам. Однако отсутствие достаточной информации не означает, что их не существует. Скорее, подтвержденная связь не может быть установлена из-за ограничений в доступных данных, чтобы прояснить, что повлекло за собой взаимодействие. Тем не менее, принимая во внимание подтвержденное использование торговых площадок даркнета злоумышленниками, наблюдаемые призывы к действию в отношении кибератак и возможности для совершения киберпреступлений, можно сделать вывод, что они действительно служат инструментами, используемыми террористами и их сторонниками для реализации стратегий кибератак, особенно когда в них замешан компонент мошенничества или отмывания денег.

Независимые домены dark web (.onion). Было замечено, что злоумышленники создают свои собственные скрытые сервисы в даркнете, используя независимые домены (.onion). Их цели широкомасштабны, террористические группы и группы ненависти в целом используют их для распространения новостей и пропаганды, примерами являются официальные публикации базирующегося в Афганистане «Исламского государства»[1] в провинции Хорасан (ISKP) и американский неонацистский сайт «The Daily Stormer». Злоумышленники также были замечены в использовании этих доменов для размещения блогов, предоставляющих дополнительную информацию об их деятельности, и для хранения украденных данных.

В отличие от рынков даркнета, которые, как правило, публикуют URL-адреса на информационных сайтах и форумах даркнета, злоумышленники обычно публикуют свои URL-адреса даркнета на поверхностном вебе, в глубинном вебе, на зашифрованных коммуникационных платформах, таких как Telegram, или на специализированных форумах по киберпреступности даркнета. Кроме того, контент на этих доменах часто не является эксклюзивным для даркнета, и копии информации часто можно найти в других местах преступного мира.

Предполагается, что причиной использования независимых доменов даркнета может быть предоставление альтернативного варианта для пользователей, которые предпочитают защиту, предлагаемую даркнетами. Также считается, что использование этих сайтов обеспечивает постоянный доступ, поскольку поставщикам платформ и правоохранительным органам становится сложнее вывести информацию в офлайн.

Форумы по киберпреступности. Подобно рынкам даркнета, существует множество криминальных форумов, расположенных в даркнете, предоставляя пространство для различных субъектов угроз для обмена информацией, торговли нелегальными продуктами и услугами и общения с единомышленниками. Подобно независимым доменам, эти платформы часто бывают зеркальными как в глубокой сети, так и в даркнете, выступая в качестве удобных цифровых мест встречи для субъектов угроз во всем преступном мире.

В отличие от рынков даркнета, ориентированных на торговлю различными незаконными товарами, криминальные форумы обычно демонстрируют более специализированную направленность. Это особенно очевидно в сфере киберпреступности, примером чему слу-

[1] Террористическая организация, запрещенная в Российской Федерации.

жат форумы, ориентированные на киберпреступность, такие как Breachforums, XSS.in и Exploit.in. Эти форумы предоставляют такие возможности, как обмен техническими знаниями, сетевое взаимодействие, доступ к руководствам по взлому, продажа скомпрометированных кредитных карт, взломанных данных, а также продуктов и услуг киберпреступности.

Форумы киберпреступности широко используются злоумышленниками, движимыми как финансовыми, так и другими мотивами. Их популярность можно объяснить доступом, который они предоставляют в соответствии с продолжающейся эволюцией возможностей кибератак, и ролью, которую они играют в повышении технической компетентности. Форумы также могут служить платформами для транзакций, и некоторые администраторы, например, администраторы Blackforums — популярного варианта для нефинансово мотивированных субъектов угроз — также предположительно управляют собственными сервисами, такими как торговые площадки Telegram и защищенные хостинговые сервисы. Кроме того, криминальные форумы, публично предоставляющие персонально идентифицируемую информацию, позволяют обмениваться личными сообщениями и использовать более ограниченные каналы связи, где могут происходить подробные обсуждения и конфиденциальное планирование атак. Однако, как и на торговых площадках «темной паутины», отсутствие видимости этих ограниченных слоев затрудняет возможность делать существенные выводы, хотя более широкое использование форумов киберпреступности субъектами угроз с мотивами, отличными от финансовых, очевидно.

Возможности шифрования и обеспечения конфиденциальности. Субъекты угроз становятся все более технически осведомленными и заботящимися о безопасности в сети. Продвижение VPN активно поощряется субъектами угроз, использующими даркнеты, в то время как другие, по-видимому, уверены в своей способности сохранять анонимность, не полагаясь на Tor. Следовательно, субъекты угроз стали более активными на зашифрованных коммуникационных платформах, а Telegram изображается как быстро появляющаяся «новая темная паутина» для кибератак в более широком киберпреступном подполье. Однако отмечается, что особенно террористические группы, по-видимому, готовы открыто общаться на публичных каналах Telegram. Хотя эта открытость способствует возникновению интереса к их делу и подстрекательству к дальнейшей активности, она также показывает

меньшую обеспокоенность по поводу обнаружения и необходимости в даркнетах для маскировки их деятельности.

Исследования также освещают дискуссии в кругах нефинансово мотивированных субъектов угроз относительно других возможностей шифрования на основе Tor, таких как Decentra, менеджер ботов на основе Tor для незаконной рыночной деятельности, а также продвижение GetTor, браузера Tor, через каналы Telegram. Аналогичным образом распространенность анонимных почтовых серверов на основе Tor очевидна, и внимания заслуживает Mail2Tor, поскольку анонимные службы обмена файлами или почтовые серверы играют решающую роль в методах, используемых некоторыми субъектами угроз. Например, было установлено, что субъекты угроз, участвующие в атаках на критически важную инфраструктуру, используют различные платформы, такие как Anonymfile, Mega.nz и Catbox, для обмена информацией. Более того, сообщалось, что функции обмена файлами Discord сами по себе позволяют злоумышленникам осуществлять атаки с использованием зараженных файлов. Исследования также подтвердили случаи использования злоумышленниками общедоступных облачных сервисов, таких как Dropbox, Google Drive, Microsoft One Drive и Amazon Cloud Drive.

Криптовалюты. Криптовалюты стали основополагающим элементом киберпреступности и служат финансовой основой для киберпреступности как услуги. Децентрализованные сети и воспринимаемая анонимность делают их предпочтительным методом как для финансово, так и для нефинансово мотивированных субъектов угроз. Они облегчают целый ряд действий, от покупки и продажи продуктов и услуг для кибератак до обеспечения других форм финансирования терроризма и отмывания денег. Более того, сама криптовалюта может быть конечным товаром в кибератаках, осуществляемых с целью финансирования терроризма.

Хотя экосистема криптовалюты широка и охватывает цифровое пространство, всплеск криптовалюты как услуги наблюдается в «темной паутине», в частности обмен монетами, кросс-чейн-мосты и сервисы смешивания. Отсутствуют исчерпывающие данные, позволяющие установить, в какой степени субъекты угроз используют эти конкретные сервисы и является ли это целями кибератак. Тем не менее существующие исследования действительно предполагают различимую закономерность. Расширяются инициативы по финансированию терроризма, охватывающие более 30 различных криптовалют, многие из которых используются в мероприятиях по сбору средств. Бо-

лее того, деятельность субъектов угроз выходит за рамки нескольких блокчейнов. На Форуме новых технологий Интерпола в октябре 2023 г. компания Merkle Science представила результаты, согласно которым на долю TORN пришлось около 90% средств, связанных с финансированием терроризма с 2021 г. Характер использования в сочетании со степенью их доступности в даркнете и важностью криптовалюты как инструмента киберпреступности позволяет предположить: весьма вероятно, что эти сервисы используются. Это открывает значительные возможности для расследований, учитывая растущую эффективность аналитических инструментов блокчейна и криптовалюты.

§ 9. Кибертерроризм и 3D-печать

3D-печать подобно Интернету приносит в жизнь наряду с новыми возможностями и новые риски. Одним из самых острых вопросов является способность 3D-принтера производить огнестрельное оружие. К. Уилсон, 26-летний бывший студент, анархист и либертарианец, поклонник Страшного пирата Робертса, создал проект «Wiki-оружие». Он соединил его с биткойном, разместил в темном вебе и организовал распределенную онлайн-сеть по проектированию, дизайну и печати на 3D-принтере различных образцов оружия.

Его крупнейшим достижением стали автоматическая винтовка, которая смогла сделать 600 выстрелов, и боевой пистолет, стреляющий стандартными пулями. Отвечая на вопросы в прессе, зачем он это сделал, Уилсон сказал: «Компьютер, Интернет и 3D-принтер дали мне возможность реализовать американскую Конституцию, предусматривающую право граждан вооружаться».

Пластиковое огнестрельное оружие особо опасно, поскольку незаметно для стандартных детекторов безопасности, установленных в правительственных зданиях, аэропортах и т. п. Лишний раз это доказала команда израильских отставных военных, которые два раза подряд пронесли в хорошо охраняемое и защищенное поясами безопасности здание Кнессета напечатанный на 3D-принтере пистолет.

Такой пистолет можно легко утилизировать — достаточно сжечь орудие преступления, и никаких следов его существования не останется. А самозарядная винтовка Shuty, созданная американским энтузиастом под ником Derwood, положила начало эпохе автоматического и полуавтоматического оружия. Теперь такие устройства способны выдержать от 10 до 30 выстрелов и не расплавиться. Чисто теоретически для изготовления самострела подойдет любой, даже простейший FDM-принтер, т. е. устройство, печатающее пластиковым прутком. Это самая доступная, а потому и самая распространенная технология 3D-печати.

Аналитический центр ФБР крайне обеспокоен тенденцией производства 3D-оружия и недавно скупил все существующие модели 3D-принтеров, чтобы исследовать, какие из них террористы могут использовать для изготовления самодельного огнестрельного оружия и взрывных устройств. Уже сегодня сложные промышленные принтеры, которые тем не менее продаются всем платежеспособным клиентам, позволяют изготовить не только мелкое, но и крупное оружие, включая основные детали для пусковых установок ракет «земля — земля» и «земля — воздух».

В условиях цифрового производства инспекция на государственной границе становится бессмысленной. Если можно просто напечатать пушки, пистолеты, бомбы, то зачем переходить границы и рисковать? 3D-печать ставит принципиально новые вопросы перед международной безопасностью. Надо понимать, что в условиях миниатюризации производства, многофункциональных роботокомплексов и 3D-печати больше невозможно будет устанавливать эмбарго на поставку оружия или чего-то подобного в те или иные регионы.

Раздел III
ПРЕСТУПНИКИ И ДЕВИАНТЫ ЦИФРОВОГО МИРА

Глава 5. Хакеры и иные девианты цифрового мира

§ 1. Хакеры

Хакеры — это основная категория преступников и девиантов в цифровой среде.

Почему не всех хакеров следует называть преступниками? Дело в том, что в 60—70-е гг. XX в. хакерами называли программистов, которые исправляли ошибки в программном обеспечении каким-либо быстрым или элегантным способом. Английское слово «hack» пришло из лексикона хиппи, в русском языке есть идентичное жаргонное слово «врубаться» или «рубить в чем-то». Начиная с конца XX в. в массовой культуре появилось новое значение этого слова — «компьютерный взломщик», программист, намеренно обходящий системы компьютерной безопасности.

О. Б. Скородумова в развитии субкультуры хакеров выделяет ряд этапов[1].

Первый (60-е гг. XX в.) характерен установками на новаторский подход к исследованию программ, провозглашением принципа неограниченного бесплатного доступа для всех к информации, ценностей абсолютной свободы. На начальном этапе развития глобальной сети Интернет хакерское движение не носило деструктивного характера, отражало тенденцию творческого новаторства, исследования пределов систем, их потенциальных возможностей. Экспериментирование не преследовало достижения корыстных целей или нанесения ущерба. В этот период для сообщества хакеров, куда входили студенты и профессора крупнейших университетов и научно-исследовательских центров США, характерны дух взаимного сотрудничества, демократизм, собственный четко обоснованный этический кодекс. Важнейшая особенность субкультуры хакеров на данном этапе — представление

[1] См.: *Скородумова О. Б.* Хакеры как феномен информационного пространства // Социологическое исследование. 2004. № 2. С. 70—79.

о собственной избранности, элитарности. Многие из них оценивали себя как первопроходцев, создающих новое общество, основанное на ценностях глобального киберпространства.

Второй этап (конец 70-х гг. — начало 80-х гг. XX в.) — переход от новаторского исследования к несанкционированному вторжению в чужие системы, повышение агрессивности, использование знаний в целях протеста, удаление или изменение важных данных, распространение компьютерных вирусов и т. п. Для обозначения этой категории хакеров используется термин *кракер* (англ. cracker — взломщик) — лицо, изучающее систему с целью ее взлома. Именно кракеры реализуют свои криминальные наклонности в похищении информации и написании разрушающего программного обеспечения. Они применяют различные способы атак на компьютерную систему, используя принципы построения протоколов сетевого обмена. Техническими и социально-экономическими причинами являлись: доступность компьютера широкому кругу лиц, в том числе и программистам-любителям; ужесточение конкуренции среди компьютерных фирм; машинная и программная несовместимость, ведущая к объективной потребности во взломе и доработке программ; повышенное внимание средств массовой информации к фактам взлома систем и создание ореола «героя» вокруг взломщика.

В зависимости от мотивов деятельности хакеров для этого этапа выделяются следующие группы:

— *«белые» хакеры* — малочисленная группа, оказывающая помощь программистам и пользователям в совершенствовании управления компьютером и виртуальными сетями, модернизации и создании новых программ, борьбе с «черными» хакерами;

— *«черные» хакеры*, или кракеры, занимающиеся несанкционированным доступом к сетям и информации.

В зависимости от целей деятельности в кракерской среде выделяются следующие группы:

— *вандалы*, главная цель которых — взломать систему для ее дальнейшего разрушения;

— *шутники* — действуют для достижения известности путем взлома компьютерных систем и внесения туда различных юмористических (с их точки зрения) эффектов;

— *взломщики* — профессиональные кракеры, действуют с преступной целью кражи или подмены хранящейся информации;

— *пираты* — воруют свежие программы с помощью средств, самостоятельно разработанных или заимствованных у взломщиков, и обладают определенной специализацией: пираты-взломщики — взла-

мывают компьютерную защиту; пираты-курьеры — копируют ворованное программное обеспечение на свой компьютер; пираты-дистрибьюторы — занимаются распространением ворованного программного обеспечения;

— *шпионы* — охотятся за секретной информацией;

— *кардеры* — используют чужие (ворованные) кредитные карты для электронной оплаты товаров или услуг;

— *фишеры* — интернет-мошенники, выдающие свои страницы за сайты других;

— *фрикеры* — осуществляют взлом телефонных автоматов и сетей, обычно с целью получения бесплатных звонков или связи с Интернетом;

— *спамеры* — занимаются формированием и рассылкой непрошеной корреспонденции рекламного характера и обладают внутренней специализацией: спамеры-кракеры — создают программы для сбора адресов компьютеров пользователей с сайтов и форумов и превращения их в машины для рассылки спама; спамеры — собиратели баз данных — обслуживают нужды рассыльщиков и собирают для них почтовые адреса, которые объединяют в базы адресов; спамеры службы рассылок — рассылают спам.

В качестве социальной базы индустрии, обслуживающей кракеров, традиционно выступают:

— *клаберы* (постоянные посетители компьютерных клубов);

— *геймеры* (любители компьютерных игр) как агенты, разносящие вирусосодержащее программное обеспечение и спам[1].

Третий этап (80—90-е гг. XX в.) — стремление к созданию организованных структур, сращивание хакерской субкультуры с криминальным миром.

В этот период хакерское движение становится мощной силой, способной дестабилизировать общественные структуры, превращается в один из объектов изучения правоохранительными органами.

Хакеры точно рассчитывают рациональность методов взлома защиты компьютерной системы, разрабатывают программы действий, обеспечивающих анонимность атаки, никогда не действуя под собственным именем и тщательно скрывая свой сетевой адрес. Мировоззренческое обоснование взлома — отличительная черта хакеров этого периода. Наиболее распространенными становятся следующие виды

[1] См.: *Масленченко С. В.* Субкультура хакеров как порождение информатизации общества: дис. ... канд. культурологии. СПб., 2008; *Леви С.* Хакеры: как молодые гики провернули компьютерную революцию и изменили мир раз и навсегда. М., 2023.

атак: на системы управления базами данных, на операционные системы и сетевое программное обеспечение.

Хакеры широко применяют методы социальной инженерии, уделяя повышенное внимание манипулированию людьми и созданию программируемой модели поведения человека, о чем свидетельствует «обмен опытом» на хакерских сайтах. Они используют и целенаправленно формируют факторы, способные привести к сознательному или неумышленному соучастию в разрушении систем информационной защиты организации: неудовлетворенность сотрудника (сотрудников) социальным статусом или материальным положением; формирование политико-идеологических, нравственных, религиозных, бытовых ориентаций, противоречащих установкам фирмы; создание экстремальных ситуаций на личностном (семейном, сексуальном, финансовом и т. д.) уровне; давление на субъекта путем шантажа или обмана; имитация ранговых различий с целью получения необходимой информации; воздействие на психофизические и физиологические системы организма с использованием гипноза, психотропных препаратов, наркотиков и т. п.

Четвертый этап (конец 90-х гг. XX в. — начало XXI в.) — институализация хакеров: создание крупных объединений, союзов, фирм, тесным образом сотрудничающих с криминальными и теневыми структурами.

Активизировано взаимодействие хакеров с мафиозными структурами и террористическими организациями. Сформировался и развивается *особый вид бизнеса — аренда хакеров*, хакерство как услуга.

Топ-5 хакерских группировок мира в 2025 г. *Группировка LockBit* остается лидером в мире программ-вымогателей. С 2019 г. ее члены атаковали тысячи компаний, шифруя данные и требуя выкуп. В 2023 г. их жертвами стали более 40% всех организаций, пострадавших от подобного вымогательства. Их «фишка» — подписная модель: они продают свое программное обеспечение другим хакерам. Суммы выкупа порой достигают миллионов долларов. В 2025 г. LockBit продолжала совершенствовать свои инструменты, оставаясь кошмаром для IT-отделов по всему миру.

Lazarus Group — группировка, предположительно спонсируемая правительством Северной Кореи. Она прославилась дерзким ограблением банка Бангладеш в 2016 г. через систему SWIFT, украв 81 млн долл. США, и атакой WannaCry в 2017 г., которая парализовала системы по всему миру. Цель — финансирование режима Ким Чен Ына через кибергрaбления и шпионаж. В 2025 г. Lazarus активно ата-

ковала криптовалютные платформы, зарабатывая миллионы на краже цифровых активов.

REvil (Ransomware Evil) — еще одна звезда мира вымогателей. Громкий успех этой группировки — атака на JBS, крупнейшего производителя мяса, в 2021 г., за что компания заплатила 11 млн долл. США. В 2025 г. REvil вернулась с новыми силами после временного затишья, связанного с арестами участников. Они атакуют все: от tech-гигантов до больниц, требуя баснословные суммы. Их стиль — дерзость и публичность, они любят хвастаться своими «подвигами» в даркнете.

Anonymous — имя, которое звучит как символ борьбы за свободу, но за этой маской скрывается темная сторона. С 2003 г. эти «хакеры с идеологией» позиционируют себя борцами против системы, но их действия — это хаос и разрушения. Взломы сайтов правоохранительных органов Миннеаполиса в 2020 г. или атака на PlayStation Network в 2011 г. оставляют после себя утечки данных, миллионные убытки и пострадавших пользователей. В 2025 г. они продолжали рушить все подряд, прикрываясь лозунгами, но итог один — никакой пользы, только вред и неуправляемый беспорядок.

ALPHV, или BlackCat, — относительно молодая группировка, но она входит в топ благодаря своей изощренности. Ее программа-вымогатель считается одной из самых сложных в мире. BlackCat атакует промышленные компании, энергетику и здравоохранение, вытянула более 100 млн долл. США у 1500 жертв по данным ФБР. Ее сила — в сотрудничестве с другими группами и мощной инфраструктуре, что делает ALPHV восходящей звездой киберпреступности.

Названные группировки используют передовые технологии: от ИИ и дипфейков до уязвимостей нулевого дня. Их мотивы разные — деньги, шпионаж, идеология, — но результат один: миллиардные убытки и хаос.

§ 2. Хактивисты

Хактивисты — это одна из разновидностей хакеров, преследующих не меркантильные, а политические цели.

Хактивизм (англ. hacktivism — от слияния «хакер» и «активизм») — использование компьютеров и компьютерных сетей для продвижения политических идей, свободы слова, защиты прав человека и обеспечения свободы информации.

Исследователь хактивизма Ф. Паже полагает, что свои идеи это движение черпает из политического активизма, для которого характерен акцент на акциях прямого действия. Примерами таких акций могут служить действия членов «Гринпис», выходящих в открытое море, чтобы помешать ведению китобойного промысла; мирный захват парка в центре Нью-Йорка тысячами активистов по призыву организации Adbusters в рамках «Захвати Уолл-стрит» в июле 2011 г.

Если добавить к политическому активизму сетевую активность хакеров (действующих как с добрыми, так и со злыми намерениями), мы получим хактивизм. Существует мнение, что английское слово «hacktivism» впервые было использовано в статье Дж. Сэкаг, опубликованной в InfoNation в 1995 г. В 1996 г. этот термин появился в статье, опубликованной в Интернете членом американской группы Cult of the Dead Cow (cDc). В 2000 г. О. Раффин, другой член этой группы, написал, что хактивисты используют технику для защиты прав человека. Многие активисты, разделяющие либертарианские идеалы (стремление к сохранению свободы предпринимательства, гражданских свобод, свободы слова и свободы обмена информацией), выступают также в защиту свободы Интернета. Олицетворением хактивизма является *движение Anonymous.* С самого начала акции участников Anonymous были направлены на защиту своего понимания того, каким должен быть Интернет. Со временем они расширили свои формы борьбы, перейдя от интернет-акций к уличным протестам.

Ф. Паже выделяет в хактивизме три основные группы:

1) Anonymous — самая освещаемая в СМИ составляющая движения. Члены этой группы известны своей поддержкой свободы Интернета и выступлением против всех, кто, как они считают, мешает обмену информацией. К используемым ими методам относятся, как правило, взлом (включая DDoS-атаки), а также кража и распространение личной и (или) конфиденциальной информации. Они любят низкопробные шутки, и порой даже кажется, что они не преследуют никаких политических целей;

2) киберзахватчики — настоящие активисты. Они используют Интернет и социальные сети прежде всего для завязывания контактов, а также для пропаганды и распространения информации. К ним относятся кибердиссиденты, которые, как и их аналог в реальной жизни, больше не признают легитимность той политической власти, которой их заставляют подчиняться. Предпринимая попытки проведения крупных акций в Интернете, они надеются укрепить демократию и бороться с коррупцией в своих странах;

3) кибервоины, или патриоты, которые объединяются в «кибер-армии», процветающие во многих странах с тоталитарными тенден-

циями. Если верить их словам, то, поддерживая национальные и экстремистские движения, они действуют по поручению государственных органов своих стран. Основным методом их борьбы является искажение внешнего вида веб-сайтов. Помимо этого они делают все возможное для борьбы с диссидентами, используя для этого DDoS-атаки[1].

Подобно тому как некоторые активисты нелегально проникают на территорию атомных электростанций и другие объекты частной собственности, хактивисты нелегально проникают в частные цифровые зоны. Из-за отсутствия внутренней структуры некоторые проводимые хактивистами операции не выходят за пределы низкопробных шуток, а есть и такие, которые могут быть связаны с мафиозной деятельностью (например, с кражей банковских данных). Подобные хакерские акции нередко имеют сомнительную ценность и сложны для понимания. Такая явная беспорядочность в выборе целей заставляет предположить, что некоторые из хактивистов ведут двойную игру, используя маску политического хактивизма для прикрытия противоправных действий. «Белые» хакеры отмечают: неэтичный характер многих операций заставляет предположить, что некоторые хактивисты, возможно, действуют по указке разведслужб ряда государств[2].

Хактивизм — как связанный с деятельностью Anonymous, так и не связанный с ней, — стал значительным явлением современного мира. Преступники поняли, что Интернет может стать одним из основных плацдармов для их деятельности, а интернет-пользователи открыли для себя тот факт, что Интернет может стать общим пространством для организации протестов. В 2010 и 2011 гг., следуя примеру группы Anonymous, к тому времени уже взявшей на вооружение данную концепцию, хактивисты развили бурную деятельность.

Ж. Носетти и Е. Черненко в записке Валдайскому международному дискуссионному клубу «Кибербунт, которого нет (пока)» (июнь 2017 г.) писали, что в 2010—2011 гг. поднялся глобальный хактивистский бунт. Тогда тысячи хакеров, да и обычных пользователей со всего мира, объединили свои усилия, чтобы отомстить властям США и ряда других стран за давление на WikiLeaks. Основатель WikiLeaks Дж. Ассанж многими воспринимался как главный борец за свободу слова, а его детище — как символ новой эпохи, при которой государства не смогут утаивать информацию от граждан. Возмущенные утечкой в

[1] См.: *Paget F.* Hacktivism: Cyberspace has become the New Medium for Political Voices. McAfee Labs, 2014.

[2] Там же.

Сеть сотен тысяч секретных документов власти США пытались заставить компании отказаться от сотрудничества с WikiLeaks. Под давлением Вашингтона контракты с порталом разорвали несколько крупных платежных систем и хостинговых сервисов. Дж. Ассанжу стало куда сложнее принимать пожертвования и поддерживать доступность портала.

За WikiLeaks вступилось хактивистское движение Anonymous. К рубежу 2010—2011 гг. оно уже существовало несколько лет, но было известно лишь в узких кругах — в основном за счет нескольких успешных взломов электронных ресурсов Саентологической церкви, а также активными действиями в поддержку торрент-трекера Pirate Bay («Пиратская бухта»). Объявив о начале Operation Payback (операции «Возмездие»), они стали собирать под своими знаменами тысячи неравнодушных пользователей со всего мира. Их девизом стали слова Дж.-П. Барлоу, одного из создателей правозащитной организации Electronic Frontier Foundation («Фонд электронных рубежей»): «Первая серьезная информационная война началась. Поле битвы — WikiLeaks. Солдаты — это вы».

Принять участие в наступлении на недружественные WikiLeaks сайты мог каждый желающий: пошаговые инструкции по тому, как осуществить DDoS-атаку при помощи простой программы (Low Orbit Ion Cannon, LOIC, «Низкоорбитальная ионная пушка»), распространялись в тематических чатах и в сети микроблогов Twitter. В итоге к атакам на сайты MasterCard, Visa, Paypal и Amazon присоединились пользователи со всех континентов. Абсолютное большинство из них никогда раньше хакерством не занимались.

Массовость обеспечила успех кампании — несколько правительственных и коммерческих ресурсов удалось на время вывести из строя. В 2012 г. американский журнал Time включил Anonymous в список ста наиболее влиятельных людей года.

Многие эксперты тогда сочли, что хактивизм будет только набирать обороты и что впредь политически мотивированные пользователи будут подобным образом реагировать на любую несправедливость. Однако вскоре эта волна стихла и в таком масштабе больше не повторялась.

Ж. Носетти и Е. Черненко считают, что причин тому, что за первым кибербунтом не последовали другие, несколько. Во-первых, у движения Anonymous не было лидера или хотя бы некоего ядра, которое взяло бы на себя координацию совместных действий и мотивировало участников на продолжение борьбы. В прессе от имени движения

мог выступить любой из его членов. В чатах, где обсуждались цели и время атак, также все происходило довольно хаотично, а после первых успешных диверсий там начались ожесточенные споры относительно дальнейших мишеней. В то время как большинство «анонимов» с Запада продолжали дисциплинированно атаковать сайты отказавшихся от сотрудничества с WikiLeaks платежных систем, среди русскоязычных хактивистов начали раздаваться призывы «ударить по Пентагону».

Во-вторых, многие из тех, кто изначально симпатизировал Ассанжу, вскоре разочаровались в нем. Одних отпугнули предъявленные ему обвинения в сексуальных домогательствах. Других смутило, что WikiLeaks начали один за другим покидать ключевые сотрудники, обвинившие Ассанжа в нецелевом расходовании многомиллионных пожертвований. Третьи не согласились с решением Ассанжа выкладывать в Сеть секретные документы «без купюр», т. е. со всеми именами и адресами, несмотря на то, что это создавало угрозу жизни для некоторых из упомянутых лиц (например, информаторов американских войск в Афганистане).

В-третьих, как только Anonymous начали активно рекрутировать сторонников в Facebook[1] и Twitter, их аккаунты были заморожены, а несколько их сайтов (например, anonops.net) сами подверглись атаке и надолго «легли на дно». Лишенные площадки для общения «анонимы» долго не могли собраться с силами. Среда, благодаря которой хактивисты появились на свет, оказалась их ахиллесовой пятой.

Наконец, угасанию бунта явно способствовало преследование членов движения со стороны правоохранительных органов США. После нескольких громких арестов и показательных судебных процессов количество желающих поучаствовать в атаках заметно поубавилось. Примечательно, что действия хактивистов осудил и их кумир Дж.-П. Барлоу, назвавший DDoS-атаки «ядовитым газом киберпространства»[2].

Anonymous осуществили еще несколько «операций», уже не связанных с WikiLeaks, однако ни одна из них не была столь успешной, как «Возмездие». Сегодня под брендом Anonymous действует несколько разрозненных хакерских группировок, однако они все больше занимаются взломами «just for the lulz» — ради развлечения.

Угасание первой волны хактивизма не означает, что не будет второй и третьей. Судьба этого общественного феномена будет во многом

[1] Принадлежит компании Meta, признанной экстремистской организацией и запрещенной в Российской Федерации.

[2] См.: Валдайские записки. 2017. Июнь. № 68.

зависеть от того, найдется ли такой же мощный объединяющий фактор, каким в свое время было желание поддержать WikiLeaks и тем самым отстоять свое право на доступ к информации. Можно предположить, что при наличии общей цели объединить людей в следующий раз будет даже проще, поскольку они уже знают, каких результатов можно добиться сообща. И не факт, что бунтовщики ограничатся одними лишь DDoS-атаками[1].

§ 3. «Группы смерти» в Интернете

Клубы самоубийц существовали с древнейших времен во многие исторические эпохи: в Древнем Египте при Клеопатре, в Германии 1819 г., в Вене 1824 г., в США начала XX в. Но виртуальные сообщества сторонников суицида отличаются от своих традиционных предшественников многочисленностью, отсутствием географической привязанности и свободным доступом лиц любого возраста. Эта проблема носит общемировой характер — виртуальная культура суицида появилась практически одновременно с развитием Интернета и распространяется по миру одновременно с ним. Исследования показывают, что большинство посетителей форумов и сайтов о самоубийстве моложе 25 лет. Некоторые индивиды состоят сразу в нескольких виртуальных сообществах, посвященных суицидам. Формально это закрытые группы, но для получения допуска к информации в них необходимо просто подписаться на группу или написать о своих переживаниях редактору сайта или создателю группы в социальной сети.

Период от возникновения суицидальных мыслей до попытки их реализации называют пресуицидом: индивид находится в состоянии угнетающего аффекта, его мрачные мысли усиливаются, неудовлетворенность жизненными условиями растет. Материалы, размещенные на личных страницах в социальных сетях участников виртуальных клубов самоубийц, показывают, что они испытывают депрессию и страдают от одиночества. Такое настроение является благоприятной почвой для внушения и развития угнетающего настроения, характерного для пресуицидального периода.

В Интернете легко найти информацию о способах и местах совершения суицида. Контент виртуальных клубов самоубийств направлен на доведение его участников до суицида. Опасность открытого доступа индивида к подобной информации подчеркивает рекомендация Всемирной организации здравоохранения: нельзя публиковать в сред-

[1] См.: Валдайские записки. 2017. Июнь. № 68.

ствах массовой информации фотографии и предсмертные записки самоубийц, а также сообщать о конкретных способах совершения суицида.

§ 4. Сетевые «тролли» и иные группы травли в Интернете

Троллинг (англ. trolling) — форма социальной провокации или издевательства в сетевом общении, использующаяся как персонифицированными участниками, заинтересованными в большей узнаваемости, публичности, эпатаже, так и анонимными пользователями без возможности их идентификации.

Прямую аналогию из обычной жизни для явления троллинга подобрать нелегко. Ближайшие понятия — это искушение, провокация и подстрекательство, т. е. сознательный обман, клевета, возбуждение ссор и раздоров, призыв к неблаговидным действиям.

Термин «троллинг» (дословно — «ловля рыбы на блесну») происходит из сленга участников виртуальных сообществ. В наиболее общем виде — это процесс размещения на виртуальных коммуникативных ресурсах провокационных сообщений с целью нагнетания конфликтной обстановки путем нарушения правил этического кодекса интернет-взаимодействия. В качестве таких действий могут выступать волны правок — искажение первичных текстов (постмодерация сообщений, тем, новостей) — флейм (англ. flame — пламя, огонь) либо бесцельная конфронтация — холивары (англ.: holy war — священная война).

Основными местами осуществления троллинга могут выступать различные тематические форумы, конференции, социальные сети, порталы, чаты и новостные сайты.

В отношении пользователя, осуществляющего троллинг, утвердилось обозначение «тролль». Это слово приобрело популярность из-за другого его значения — существо, упоминаемое в скандинавской мифологии. Мифологические тролли, особенно в детских рассказах, изображаются уродливыми, неприятными существами, созданными для причинения вреда и сотворения зла. Тролль представляется типичным пользователем, который разделяет общие интересы и проблемы группы либо сообщества.

Оксфордский словарь английского языка впервые упоминает троллинг в связи с Интернетом в 1992 г., называя две версии происхождения: мифологическую и рыболовную.

С начала XXI в. интернет-тролли начали создавать *собственные сетевые сообщества* и организации для обмена опытом по наиболее эффективному разжиганию конфликтов. Первое упоминание троллинга в академической литературе произошло в 1996 г. и принадлежит Дж. Донат, которая описала троллинг как умышленно вредоносную ложь, отмечая, что тролли способствуют быстрому снижению доверия и терпимости к чужакам, а также способствуют развитию паранойи в онлайн-сообществе.

О том, почему люди занимаются сетевым троллингом, У. Филлипс в книге «Трололо»[1] пишет: помимо самоидентификации как таковой тролли мотивированы тем, что называют лулзами. *Лулзы* (англ. lulz) — особая разновидность несочувственного, трудно истолковываемого посторонними смеха. Они напоминают немецкое понятие «Schadenfreude», которое можно приблизительно перевести как «радость от несчастий кого-то вам неприятного». Но зубы у лулзов гораздо острее. Лулзы также свидетельствуют о специфической комической и визуальной эстетике.

Утверждение (и очень распространенное в мире троллей), что перед лулзами все равны, опровергается тем фактом, что значительная доля лулзов направлена на небелых (особенно афроамериканцев), женщин, а также на лесбиянок, геев, бисексуалов, трансгендеров и квир-индивидов (ЛГБТК). При этом исторически доминирующие группы также часто являются источником лулзов. «Белые христиане», и республиканцы особенно, наряду с группами белых людей, объединенных общим делом (в первую очередь это экологи и сообщества фанов), вызывают изрядное количество троллинга. Хотя на первый взгляд эти мишени кажутся совершенно разными, тролли выбирают жертв, руководствуясь общим принципом — пригодностью для эксплуатации. Тролли считают, что ничто на свете не следует принимать всерьез, и потому расценивают публичные проявления сентиментальности, политических убеждений и (или) идеологической ограниченности как призыв к троллингу.

Еще один признак троллинга — тролли настаивают на анонимности и поднимают ее как знамя. Возможность скрыть свою офлайновую личность имеет ряд важных поведенческих последствий. Самое очевидное из них — анонимность позволяет троллям совершать поступки, которые они никогда не повторили бы в профессиональной или иной публичной обстановке. И, напротив, успешность троллинга

[1] *Филлипс У.* Трололо: нельзя просто так взять и выпустить книгу про троллинг. М., 2016.

часто зависит от отсутствия анонимности мишени или по крайней мере от ее готовности раскрыть свои привязанности, интересы и уязвимые места в реальной жизни. Для троллей это основание для незамедлительного троллинга, поскольку в понимании троллей Интернет является — или хотя бы должен быть — зоной, свободной от привязанностей.

В последнее время троллинг все шире используется как PR-технология в коммерческой, политической и даже внешнеполитической сферах.

По мнению ученых из Оксфордского университета, подготовивших исследование «Войска, тролли и возмутители спокойствия: глобальный обзор организованных манипуляций соцсетями», правительства по всему миру создают «кибервойска», которые занимаются манипулированием в Facebook[1], Twitter и других соцсетях. Манипуляции в Интернете используются для управления общественным мнением, распространения дезинформации и подрыва позиций критиков. При этом согласно исследованию демократические и авторитарные режимы не слишком сильно различаются в этом отношении.

Авторы изучили ситуацию в 28 странах, где правительства применяют технологии для манипулирования общественным мнением. Речь идет о самых разных способах — как о комментировании, целевом индивидуальном подборе получаемой пользователем информации и создании спонсируемых правительством сайтов и страниц, так и о фейковых новостях и подготовке специального контента, размещаемого в соцсетях. Социальные сети делают пропагандистские кампании более сильными и потенциально более эффективными, чем в прошлом.

Правительства заимствуют применяемые в Интернете технологии и у оппозиционных активистов, которые распространяли информацию и привлекали сторонников через Интернет. При этом речь идет не только непосредственно о правительственных подразделениях, занимающихся манипулированием общественным мнением, но и о связанных с правительством партиях, организациях и частных лицах.

Есть и иные «группы травли» в Интернете, которые занимаются:

— пранком (телефонным хулиганством). Пранкер разыгрывает жертву по телефону, при этом записывает разговор и выкладывает в Интернет;

— навязчивым спамом — закидыванием жертвы сообщениями различного содержания (рекламным текстом или любым бессмысленным

[1] Принадлежит компании Meta, признанной экстремистской организацией и запрещенной в Российской Федерации.

набором слов). Цель — вывести жертву из себя потоком навязчивых сообщений;

— деанонимизацией, т. е. раскрытием имени пользователя в ситуации анонимного интернет-общения, установлением авторства какого-либо текста, рисунка вопреки желанию автора и т. д.;

— созданием групп в социальных сетях или даже сайтов, направленных против травимого;

— созданием страниц, аккаунтов от имени травимого в различных социальных сетях, журналах; пишутся (якобы жертвой) разного рода компрометирующие, грубые тексты. Это называется «атака клонов»;

— взломом учетной записи, аккаунта жертвы и рассылкой с ее страницы различной информации;

— распространением компромата, слухов, сплетен, в том числе выкладыванием различного рода личных документов, фотографий и видеороликов (нередко поддельных) в социальных сетях и т. п.;

— съемками жертвы тайком или принудительно на видео, обычно в унизительном положении, после чего запись выкладывается на YouTube или другом популярном видеохостинге.

§ 5. Деструктивные секты в Интернете

Деструктивная секта — термин, используемый социологами, психологами, криминологами, богословами по отношению к религиозным, неорелигиозным и другим группам и организациям, причинившим (причиняющим) вред обществу или своим членам (материальный, психологический или физический). Часто секты именуют *тоталитарными*, когда они обвиняются в доведении до самоубийства и убийствах людей, торговле людьми, употреблении и распространении наркотиков.

Прецеденты, когда киберпространство содействовало культовому и религиозному насилию, известны с момента появления Интернета. Так, согласно японскому изданию Japanese Newspaper Reports, когда токийская полиция изъяла множество CD-дисков из здания, принадлежащего террористической секте «Аум Синрике», в них были обнаружены длинные списки электронных адресов, принадлежавших студентам японских колледжей. Силовые структуры убеждены, что секта могла использовать свыше 40 тыс. email-контактов для вербовки новых членов из числа учащейся молодежи[1].

[1] См.: *Яковлева М. Г.* Особенности представительства деструктивных сект и экстремистских религиозных организаций в Интернете // URL: http://homocyberus.ru.

Хронологически первым деструктивным культом, имевшим представительство в Интернете, стала община «Небесные врата». Общественную огласку секта получила в марте 1997 г. после коллективного самоубийства своих членов на одном из ранчо Калифорнии. Культовый суицид был приурочен к приближению кометы Хейла — Боппа, за которой, как полагали члены общины, летит космический корабль, предназначенный для того, чтобы забрать их души в межгалактическое путешествие. Примечательно, что секта «Небесные врата» имела достаточно эффектный для того времени сайт, делая информацию о жизни общины доступной для всех пользователей Интернета. Веб-страница включала множество ярких графических изображений, но основу контента сайта составляли догматы секты. В дни, непосредственно предшествовавшие массовому самоубийству членов группы, их веб-страница провозглашала: «Красная тревога. Комета Хейла — Боппа приносит конец времен». Эксперты подчеркивают, что секта «Небесные врата» не могла добиться больших успехов в распространении своих идей посредством веб-страницы в 1997 г. по причине того, что Интернет не обладал такой популярностью, как в наши дни. Однако секта во многом опередила свое время, заложив новый вектор развития деструктивной религиозности в современном мире.

Особую опасность деструктивные секты в сети Интернет представляют для несовершеннолетних.

В последние годы в России участились факты, когда подростки под воздействием сектантских сайтов (особенно сатанистских) совершают насильственные преступления.

К насильственным преступлениям, совершаемым несовершеннолетними в ритуальной форме, относятся уголовно наказуемые деяния (убийство, умышленное причинение вреда здоровью различной тяжести, побои, истязание, изнасилование, насильственные действия сексуального характера, вовлечение несовершеннолетнего в совершение преступления и антиобщественные действия, вандализм, жестокое обращение с животными и др.), совершаемые ими в процессе совместного участия в «магических» ритуалах, связанных с их приверженностью к верованиям и оккультным учениям, либо под влиянием таких приверженцев. При этом для насильственных преступлений, совершаемых в ритуальной форме несовершеннолетними, характерны коллективные формы проявления жестокости и агрессивности, порождаемые общим чувством зависимости от сверстников на фоне крушения авторитета взрослых[1].

В зависимости от целей ритуалы, сопровождающие насильственное поведение несовершеннолетних, выражаются в следующем:

— совершение жертвоприношения, в том числе человеческого;

— совершение убийства, представляющего собой ритуал мести (может совершаться в том числе и по мотиву религиозной ненависти или вражды);

— совершение насильственного преступления как части обряда посвящения в члены секты;

— совершение насильственного преступления с целью получения органов и тканей живых существ, которые необходимы для последующих ритуальных манипуляций;

— совершение насильственного преступления для «приобретения каких-либо магических способностей»;

— совершение насильственного преступления в целях «вызывания духов и демонов»;

— совершение насильственного преступления в целях гадания (обычно умерщвляется животное);

— совершение акта экзорцизма, т. е. процедуры изгнания бесов и других сверхъестественных сущностей из «одержимого» с помощью молитв, обрядов определенной религии, в результате чего потерпевшему может причиняться физический вред, вплоть до смерти.

Насильственные преступления в ритуальной форме несовершеннолетние в большинстве случаев совершают группой лиц по предварительному сговору, чаще организованной группой. Численный состав может варьироваться от двух человек до 15—20 и больше. Многочисленные группы в основном имеют смешанный возрастной состав и возглавляются совершеннолетними. Каждое третье ритуальное насильственное преступление совершается подростками в отношении лица, заведомо находящегося в беспомощном состоянии, которое обусловлено малолетним возрастом, в силу чего жертва преступления не была способна защитить себя, оказать активное сопротивление виновным, которые осознавали это и рассчитывали воспользоваться этим состоянием жертвы. При этом механизм совершения насильственного преступления несовершеннолетними в ритуальной форме характери-

[1] См.: *Семочкина А. А.* Предупреждение насильственных преступлений, совершаемых несовершеннолетними в ритуальной форме: дис. ... канд. юрид. наук. М., 2016.

зуется тщательной продуманностью действий преступников, их согласованностью, последовательностью и единством[1].

Часто такие насильственные действия снимаются на видео через смартфоны и выкладываются в Сеть.

В России в 2025 г. обратили внимание на растущую волну сектантства — уже не в привычном понимании религиозных культов, а *в форме бизнес-тренингов, оккультных практик и психологических групп*. Эксперты бьют тревогу: под видом личностного роста и духовных поисков граждан массово вербуют в деструктивные сообщества, которые разрушают семьи, подрывают здоровье и угрожают национальной безопасности. Законодательство не поспевает за изощренными методами вербовки, а сами секты научились искусно маскироваться под легальные организации.

Проблема сектантства в России внезапно материализовалась, сначала обозначившись борьбой против различных оккультных вещичек с сайтов объявлений и продолжившись внезапным запретом сатанизма (как запрещенной экстремистской организации). Покончив с сатанизмом, законодатели дошли и до мелких сект, которые объединяют вокруг себя людей для целей не всегда моральных, законных и в большинстве случаев деструктивных для психики и материального положения человека.

По оценкам экспертов, только в «традиционных» сектах состоят около 1,5 млн человек, но реальные цифры могут быть кратно выше — за счет новых форм вербовки. Нет единого законодательного определения понятия «секта», потому нет системного мониторинга, а правоохранители часто не успевают реагировать на стремительно меняющиеся методы их влияния. Подсчеты разных специалистов строятся по разным моделям. Юристы исходят из фактов посягательства на права человека, психологи — из манипуляции сознанием, социологи — из изоляции человека от привычной среды. Именно поэтому цифры разнятся: если учитывать только те случаи, где есть состав преступления, то счет идет на тысячи, но если брать все формы деструктивного влияния — на миллионы.

География распространения сектантства — не только Москва и Петербург, но и другие города-миллионники — Екатеринбург, Казань, Новосибирск. Вербовка осуществляется через телеграм-каналы, игры, курсы йоги или даже маникюрные салоны. Некоторые секты координируются из-за рубежа, например Международным альянсом религиозных свобод, признанным в России нежелательной организацией.

[1] См.: *Семочкина А. А.* Указ. соч.

Секты сегодня — это часто не маргинальные сообщества, а структуры, возглавляемые образованными и вменяемыми людьми. Это хороший бизнес: можно не платить налоги, зарабатывать на людях, обожающих тебя как воплощение бога. Вербуют в основном тех, кто переживает кризис: потерю близкого, стресс на работе, одиночество.

Проблема сектантства в России требует системного ответа: не только запретительных мер, но и просвещения, поддержки традиционных конфессий, создания государственных программ мониторинга деструктивного контента. Пока же секты остаются серой зоной, где пересекаются интересы мошенников, внешних сил и внутренних лоббистов.

§ 6. Организованная преступность цифрового мира

В настоящее время согласно исследованию RAND Corporation 80% хакеров входят в состав регулярных (постоянных) организованных преступных групп. В том, что преступники используют технологии, нет ничего нового. Однако есть некая принципиальная разница между вчерашним днем и днем сегодняшним. Раньше преступники использовали военные или гражданские технологии, приспосабливая их для своих нужд. Нынешние преступные группы сами разрабатывают технологии, используют их как отдельный побочный бизнес и реализуют через свои легальные предприятия в гражданской и военной сферах.

Кроме того, особенностью современной организованной преступности является упор на исследования и разработки. Если раньше она использовала технологии либо те или иные устройства по прямому назначению, то теперь старается выжать из технологий все возможное.

Начиная с 2000 г. организационные формы серьезной криминальной деятельности претерпели значительные изменения. Сегодня они являются наиболее разнообразными и пластичными за весь период существования европейского организованного криминала.

До начала XXI в. существовало два основных типа структур организованной преступности.

Первый тип — это *жестко структурированные иерархические ОПГ*. Для этих групп характерен постоянный состав руководителей и значимых членов при достаточно высокой текучести рядовых участников групп. Как правило, в таких ОПГ вопросы решаются коллегиально, а преступный лидер выполняет функции не столько безусловного ру-

ководителя, сколько арбитра и последней инстанции при отсутствии единодушия среди руководящего состава группировки. Подобные ОПГ формировались по принципам местничества (происхождения из одной местности, города, района, пребывания в одной тюрьме и т. п.) или этнического состава (для национальных меньшинств). Если ранее такие группировки, как правило, занимались одним-двумя видами преступной деятельности, то чем дальше, тем больше они диверсифицируют свою деятельность.

Наибольшие успехи в борьбе с организованной преступностью начала XXI в. на уровне как отдельных государств, так и сообщества в целом связаны с операциями правоохранительных органов именно против этого типа ОПГ. Они наиболее распознаваемы и уязвимы. Как правило, участники этих ОПГ ни раньше, ни теперь не вовлечены в легальную экономическую деятельность и являются либо безработными, либо лицами без определенных занятий, либо скрываются от правоохранительных органов. С появлением информационного общества с новыми средствами наблюдения и контроля распознавать тип активности населения стало гораздо проще, чем ранее.

Вторым типом организационных структур преступности в странах ЕС в конце XX — начале XXI в. были *ОПГ временного характера и состава*. Эти группы в отличие от традиционной иерархически организованной преступности создавались и создаются для проведения конкретных преступных операций либо реализации определенных, относительно кратковременных — от трех месяцев до полутора-двух лет — криминальных проектов.

Подобные группы, по образному выражению М. Поттера, аналитика ФБР, являются реализацией продюсерской экономики в преступном мире. Как правило, такие группы формируются вокруг преступного лидера, имеющего высокий авторитет в криминальных кругах, проектировщика или разработчика криминальной операции (проекта) и небольшого числа высококвалифицированных опытных преступников различной функциональной специализации.

Постепенно ядро обрастает либо исполнителями подсобных работ, либо участниками, принимающими на себя основные риски возможных боевых столкновений с правоохранителями. Временные ОПГ формируются не по местническому или этническому признаку. Их состав в решающей степени зависит от личных знакомств лидера и членов функционального ядра ОПГ.

На рубеже XX и XXI вв. с приходом в Интернет не только университетов и продвинутых пользователей, но и бизнеса, и среднего класса

появились первые *киберпреступные сетевые ОПГ*, в основе организации которы лежит сетевой принцип. В отличие от традиционной организованной преступности участников ОПГ не обязательно связывают длительные личные отношения и даже просто очные знакомства. Во многих кибергруппировках такого рода личные пересечения не поощряются. При этом практически обязательным условием вхождения в состав подобных ОПГ является длительный бэкграунд в различных подпольных форумах, чатах. Кроме того, широко распространен институт рекомендателей. Для вхождения в состав сетевой ОПГ требуется, чтобы кто-то, лично знающий руководителей ОПГ, порекомендовал потенциального кандидата, с которым встречался на различных хакерских конференциях, неформальных встречах и т. п.

Принципиальное отличие блочно-сетевой структуры организованной преступности от традиционных ОПГ состоит в том, что в стабильном, устойчивом ядре аккумулируются руководство, наиболее опытные и искусные преступники, а также люди, выполняющие сервисные функции, связанные с отмыванием денег, защитой в судах, коррупционными связями с государственными структурами и т. п. Все остальные, в том числе профильные, функции подобных ОПГ выполняют специализированные по территориальному или функциональному признакам *контрактные ОПГ*, работающие по модели «преступление как сервис». Переход от иерархической к блочно-сетевой структуре усложнил работу правоохранительных органов по выявлению и пресечению деятельности руководителей преступных образований. При блочно-сетевой модели основной удар принимают на себя преступники-контрактники. При пресечении деятельности ОПГ, работающих на подряде, или при малейшем подозрении на раскрытие их деятельности правоохранительными органами блочное ядро прекращает любые контакты и заключает новый контракт с другой группой.

Наибольшие опасения вызывает появление на территории ЕС так называемых *мебиус-преступных групп*. Отличительными особенностями этих групп являются небольшая численность, легальный характер занятий участников групп, высокий уровень их профессиональной, в том числе высокотехнологической, расследовательской и военной компетенции.

Такого рода группы выполняют заказы крупных бизнес-структур, а иногда и государственных органов некоторых стран. Также они подряжаются для выполнения контрактов с террористическими группами и сетями. Такого рода группы самостоятельно разрабатывают, готовят и осуществляют технически и организационно сложные преступления.

Важнейшим направлением развития деятельности ОПГ являются их усилия по *повышению результативности отмывания преступных доходов, их трансферту в законную экономику*. Криминальные сети и группы постоянно стремятся использовать новейшие технические разработки, такие как криптовалюты и анонимные способы оплаты. Быстрая обработка транзакций и распространение эффективных инструментов анонимизации затрудняют деятельность правоохранительных органов по доказательной идентификации реальных бенефициаров доходов от преступной деятельности.

Все возрастающее количество онлайн-платформ и приложений предлагают новые способы перевода денег. Они не регулируются в той же степени, что и традиционные поставщики финансовых услуг, что облегчает жизнь преступников.

Также облегчает жизнь преступникам онлайн-банкинг. На «черном» рынке, ориентированном на ОПГ, активно продаются специальные программы, позволяющие обойти все более широко применяемую биометрическую идентификацию собственников счетов физических и юридических лиц.

Важнейшими факторами перемен в направлениях деятельности, структуры и методов организованной преступности в Европе являются *технологические инновации*. Преступники демонстрируют высокую степень приспособленности и креативности в использовании новых технологий. Интернет и возрастающие возможности его подключения ко всем компонентам физической среды оказывают все большее влияние на виды серьезной организованной преступности. Инновации в инструментарии и методах, коммуникациях и логистике криминала все в большей степени позволяют ОПГ совершать преступления анонимно, в любом месте, в любое время, без физического присутствия.

Другим ключевым фактором, определяющим изменения криминального ландшафта, является *динамика геополитической ситуации*. Организованные преступные группы уже извлекли сотни миллионов долларов преступных доходов от конфликтов на Украине и Ближнем Востоке.

Еще одним направлением развития ОПГ является *установление все более тесных связей между преступностью и корпоративным сектором* в некоторых странах. Данное взаимодействие строится по трем направлениям.

Во-первых, бизнес-структуры, иногда даже крупнейшие корпорации, не гнушаются заказывать у преступников определенные мероприятия. В наибольшей степени это имеет отношение к киберпреступности и связано с кражей интеллектуальной собственности и компрометирующей конкурентов документации.

Во-вторых, ОПГ стараются в гораздо больших размерах, чем ранее, инвестировать преступные прибыли не в криминальный, а в легальный бизнес. Особым интересом у ОПГ пользуются такие отрасли, как строительство, уборка городского мусора и экология в целом. Также криминал инвестирует в IT-индустрию, особенно в финансовые технологии, изготовление видеоигр и различного рода приложений, предусматривающих получение от клиентов персональных данных.

Наконец, в-третьих, это шантаж со стороны ОПГ среднего, крупного и особенно крупнейшего бизнеса. Шантаж основан на практике уклонения европейского бизнеса от налогообложения с отправлением денег в офшорные юрисдикции. По данным Европола, некоторая часть адвокатских, консультативных и регистрационных бюро, связанных с налоговым планированием и трансфертом средств в офшорные зоны, которыми пользуется легальный бизнес, находится под контролем международных ОПГ.

Новой чертой последних лет стало пристальное *внимание ОПГ к крупнейшим транспортным хабам*, используемым для глобального распределения товарных потоков.

В настоящее время наибольшие темпы роста преступности приходятся на локации, характеризующиеся наличием эффективной транспортной инфраструктуры, близостью или связью со странами — источниками товаров, услуг или мигрантов, доступом к деловым или инвестиционным возможностям, а также спросом на незаконные товары и услуги.

Раздел IV
ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ КАК ГЛАВНАЯ ТЕХНОЛОГИЯ ДЛЯ КРИМИНОЛОГИЧЕСКОГО АНАЛИЗА

Глава 6. Значение искусственного интеллекта для правоохранительной деятельности[1]

§ 1. Архитектура искусственного интеллекта, значимая для криминологии

В России правовое определение ИИ содержится в Национальной стратегии развития искусственного интеллекта на период до 2030 года:

«...искусственный интеллект — комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые с результатами интеллектуальной деятельности человека или превосходящие их.

Комплекс технологических решений включает в себя информационно-коммуникационную инфраструктуру, программное обеспечение (в том числе, в котором используются методы машинного обучения), процессы и сервисы по обработке данных и поиску решений».

В сентябре 2025 г. Рабочая группа Государственной Думы по разработке законопроекта о регулировании искусственного интеллекта определила ИИ как «любую систему данных, программное обеспечение (ПО) или аппаратное средство, способное обрабатывать информацию способом, напоминающим разумное поведение, с использованием

[1] В главе использованы: Доклад Интерпола и Межрегионального научно-исследовательского института ООН по вопросам преступности и правосудия (ЮНИКРИ) «Инструментарий для ответственных инноваций в области ИИ в правоохранительной деятельности» (июнь 2023 г.); Доклад Инновационного центра Интерпола «ChatGPT: воздействие на правоохранительные органы» (август 2023 г.); Отчет инновационной лаборатории Европола «Преимущества и проблемы искусственного интеллекта для правоохранительных органов» (октябрь 2024 г.); Исследование компании Robust Intelligence и Университета Пенсильвании «Оценка риска безопасности в DeepSeek» (31 января 2025 г.).

методов машинного обучения для генерации контента, прогнозов, рекомендаций или решений».

В постоянно меняющемся ландшафте правоохранительных органов ИИ появился как преобразующий инструмент, привнося возможности, которые могут полностью изменить деятельность по борьбе с преступностью. Правоохранительные органы во всем мире сталкиваются со все более сложными проблемами — от экспоненциального роста данных, генерируемых цифровыми устройствами и онлайн-сервисами, до сложной природы современной преступной деятельности. Очевидно, что традиционных методов полицейской деятельности недостаточно в качестве ответа. Более того, глобализация преступности, отмеченная киберугрозами, трансграничной торговлей людьми и международным терроризмом, представляет собой все более сложную картину, которая требует передовых и инновационных решений.

В свете этого ИИ предлагает многообещающую альтернативу. Используя самые современные технологии, правоохранительные органы могут решать многие из этих насущных проблем. Мощь ИИ в обработке огромных объемов данных и фильтрации релевантного контента, его возможности моделирования данных и его способность выявлять закономерности и тенденции, ранее не поддававшиеся обнаружению следователями-людьми, подчеркивают его преобразующий потенциал. Помимо этого, использование ИИ для повторяющихся и ресурсоемких задач позволяет правоохранительным органам работать более эффективно с их ограниченными ресурсами, а сотрудникам полиции сосредоточиться на своих самых важных задачах и расставить приоритеты.

Тем не менее это имеет свою цену, поскольку некоторые приложения ИИ в полиции вызывают опасения с точки зрения конфиденциальности, предвзятости и дискриминации. Существуют опасения, что эти сложные и несколько непрозрачные системы могут принести больше вреда, чем пользы.

Технология ИИ способна полностью преобразовать правоохранительную деятельность: от продвинутой криминальной аналитики, которая выявляет тенденции в огромных объемах данных, до биометрии, которая позволяет быстро и однозначно идентифицировать преступников.

Аналитика данных. Способность анализировать огромные объемы информации и затем оперативно принимать эффективные решения стала неотъемлемой частью цифровой эпохи. В таких областях, как правоохранительная деятельность, решения часто приходится при-

нимать в условиях ограниченных ресурсов и ограниченного времени (например, во время полицейского рейда, похищений или захвата заложников). Таким образом, ошибки при принятии решений могут иметь глубокие социальные последствия, а также негативные последствия для прав и свобод граждан.

По своей сути аналитика данных подразумевает извлечение знаний и действенных идей из необработанных и сырых данных. Она представляет собой способ выявления закономерностей, тенденций и связей в огромных наборах данных. Появление ИИ значительно расширило возможности традиционной криминальной аналитики данных. Способность систем ИИ учиться и адаптироваться на основе данных, включая исторические и другие криминальные данные, доступные правоохранительным органам, позволяет аналитикам перемещаться по огромным объемам информации, обрабатывать и анализировать их более эффективно и точно, чем любой человек мог бы это сделать без такого рода технической помощи.

Например, используя инструменты анализа на основе ИИ, следователи могут анализировать миллионы финансовых транзакций и обнаруживать аномалии, подозрительные перемещения средств, чтобы выявлять мошенничество. Для правоохранительных органов это означает улучшенную способность анализировать и понимать схемы преступлений, обнаруживать связи между международными расследованиями и разрабатывать индивидуальные стратегии для решения конкретных задач.

Эта преобразующая сила ИИ не только облегчает обработку данных, но и обогащает качество генерируемых разведданных. Например, там, где традиционная аналитика может просто указать на всплеск преступности, аналитика на основе ИИ может потенциально выявить глубинные причины, корреляции между внешними и несвязанными событиями или даже тонкие закономерности, которые остались бы незамеченными при ручном анализе. Следует отметить, что это обычно делается в целевых случаях использования в контексте хорошо подготовленных и закрытых наборов данных.

Кроме того, в криминальных областях, связанных с цифровыми устройствами, такими как смартфоны, объем данных, которые необходимо проанализировать и на основе которых необходимо действовать, огромен и сложен. В этих сценариях аналитика данных на основе ИИ становится незаменимой для эффективного анализа. Без помощи ИИ правоохранительные органы могут столкнуться со значительными трудностями при расшифровке огромных массивов данных, что приведет к потенциальным пробелам, затянутым расследованиям и упущенным возможностям поимки преступников. Например, простой просмотр объема данных, сгенерированных одним смартфоном, невозможен без технической помощи.

Большие и сложные наборы данных. Правоохранительные органы все чаще сталкиваются с проблемой навигации по большим и сложным наборам данных, которыми невозможно легко управлять и обрабатывать с помощью стандартных инструментов. Обработка таких сложных наборов данных требует специальных методов. Для хранения, обработки и доступа к огромным объемам данных часто используются передовые системы управления базами данных и масштабируемые поисковые решения, параллельная обработка и инфраструктуры облачных вычислений.

Более того, модели ИИ, включая алгоритмы машинного обучения, играют решающую роль в анализе и осмыслении этих данных, особенно когда человеческий анализ был бы слишком медленным или неэффективным.

Конечная цель навигации по большим и сложным наборам данных — извлечение полезных сведений. Для правоохранительных органов это может означать расшифровку тысяч часов аудиофайлов, извлечение таких сущностей, как имена и номера телефонов из текстовых сообщений, без необходимости просмотра содержимого сообщения; таким образом, это служит для ограничения потенциальных нарушений защиты данных и минимизирует объем обработки персональных данных. Другие соответствующие приложения в полицейской деятельности включают возможность:

— выявлять закономерности в преступной деятельности;

— выявлять корреляции между различными типами данных (например, погодными или сезонными закономерностями и уровнем преступности);

— прогнозировать потребности в ресурсах на основе прошлых тенденций (например, полицейское управление пытается определить, сколько сотрудников ему следует направить в разные участки в разное время дня и недели).

Этот список не является исчерпывающим. Новые варианты использования анализа больших и сложных наборов данных в правоохранительных органах будут появляться по мере развития технологий и изменения криминального ландшафта.

Обмен информацией между различными ведомствами и подразделениями правоохранительных органов. Фрагментированные си-

стемы данных, информационные хранилища и ограниченная совместимость между базами данных могут препятствовать всестороннему анализу больших и сложных наборов данных. Сотрудничество и обмен данными между ведомствами, а также разработка и принятие общих стандартов имеют жизненно важное значение для использования всего потенциала данных, но достижение этого на практике часто оказывается сложным.

Прогнозная деятельность. В правоохранительных органах процессы принятия решений все больше зависят от разведданных, полученных из больших и сложных наборов данных. Недавним достижением является «*прогностическая (предиктивная) полиция*», использующая сложные статистические методы для извлечения ценных новых идей из обширных наборов данных, например, по записям о преступлениях, событиям и факторам окружающей среды, выявленным в криминологии. Этот подход позволяет полицейским органам выявлять закономерности, связанные с возникновением преступлений и небезопасных ситуаций, и развертывать силы в соответствии с этими идеями для минимизации рисков.

Предиктивная полиция использует возможности ИИ для повышения эффективности и результативности деятельности. Реализуемая в первую очередь с помощью моделей машинного обучения на основе правил, предиктивная полиция включает два основных этапа: сбор данных и моделирование данных (прогнозирование). На этапе сбора данных полицейские управления накапливают структурированные и неструктурированные данные из различных источников, включая исторические данные о преступлениях (время, место и тип), социально-экономические данные и переменные возможности. В некоторых случаях эта информация дополняется данными из служб пробации и социальных служб, а также другими соответствующими источниками.

Затем алгоритмы машинного обучения используются для анализа этих данных на этапах обучения и прогнозирования. Модель ИИ выявляет закономерности в исторических данных, связывая индикаторы с вероятностью совершения преступления, а затем генерирует оценки риска в качестве прогнозных результатов.

Прогностическая деятельность полиции осуществляется в двух основных формах: территориальной и индивидуальной.

Территориальные алгоритмы выявляют связи между местоположениями, происшествиями и исторической статистикой преступлений, чтобы прогнозировать вероятность совершения преступлений в определенное время и в определенном месте. Например, они могут прогнозировать рост уровня преступности при определенных погодных условиях или на крупных спортивных мероприятиях.

Индивидуальный прогноз направлен на лиц, которые с наибольшей вероятностью будут заниматься преступной деятельностью.

Разведка с открытым исходным кодом (OSINT). Подкатегория больших и сложных наборов данных формируется из источников *разведки с открытым исходным кодом* (англ. open source intelligence, OSINT), особенно в эпоху, когда объем данных в Интернете стремительно растет.

После 2020 г. онлайн-трафик значительно увеличился. Принудительные блокировки, вызванные глобальной пандемией, способствовали всплеску числа интернет-пользователей по всему миру. Эта новая «норма» также проложила путь к всплеску киберпреступности и привела к значительному усилению пропаганды насильственного экстремизма и террористического контента в Интернете. В огромном пространстве цифрового мира, где киберпреступники действуют быстро, традиционные методы OSINT часто терпят неудачу, сталкиваясь с дилеммой «подавляющих данных, ограниченного времени». Изучение больших, разнообразных и неструктурированных наборов данных для извлечения ценных разведданных требует значительных ресурсов, таких как время, персонал и деньги — активы, не всегда доступные многим правоохранительным органам.

Импульс существенно смещается в сторону автоматизации, оптимизации использования ресурсов и повышения точности принятия решений. В сфере OSINT автоматизация помогает пользователю раскрывать и использовать ранее не использовавшиеся источники. Следовательно, все большее число мировых правоохранительных органов внедряют автоматизированные инструменты OSINT для целей расследования.

Приложения автоматизированной парадигмы OSINT безграничны — от расследования и реконструкции онлайн-следов преступников до проверки веб-приложений и обнаружения киберугроз на социальных платформах. Автоматизированные инструменты OSINT предоставляют информацию, которая усиливает расследования на ранних стадиях, помогая следователям перейти от простого реагирования к активному предотвращению.

Однако остается серьезная проблема: работа с неструктурированными данными. Чтобы справиться с этой проблемой, правоохранительные органы могут использовать автоматизированные многоисточниковые инструменты OSINT и аналитики социальных сетей (англ.

social media intelligence, SOCMINT) с поддержкой ИИ, которые способны управлять как структурированными, так и неструктурированными данными. Эти инструменты, оснащенные самообучающимися моделями машинного обучения, могут переформатировать неструктурированные данные, поддерживать целевые поиски и расследования в открытых источниках и предлагать информацию в режиме реального времени. Важно, что все это должно делаться со скоростью, превышающей скорость, с которой преступники могут стирать свои цифровые следы.

Кроме того, *поставщики онлайн-услуг и интернет-справочные подразделения* могут использовать возможности ИИ для обнаружения и противодействия террористической пропаганде, дезинформации, разжиганию ненависти и незаконному онлайн-контенту. Используя передовые алгоритмы ИИ и машинного обучения, они могут анализировать огромные объемы данных на высокой скорости для выявления шаблонов, ключевых слов или визуального контента, связанных с экстремистскими идеологиями. Более того, системы с поддержкой ИИ можно обучать на известных пропагандистских материалах, чтобы заблаговременно обнаруживать новый контент, имеющий схожие характеристики, и сообщать об этом сотрудникам правоохранительных органов, обеспечивая более оперативное и эффективное удаление вредоносного контента до его распространения.

Использование ИИ для модерации контента представляет собой сложную задачу, особенно в отношении баланса между правом на свободу выражения мнения и свободой мысли, совести и религии и необходимостью противодействовать дезинформации, разжиганию ненависти и незаконному контенту в Интернете.

Обработка естественного языка (NLP). Обработка естественного языка (англ. natural language processing, NLP) — это раздел компьютерной науки и лингвистики, который фокусируется на взаимодействии между компьютерами и человеческим языком. Он стремится дать возможность машинам интерпретировать и генерировать человеческий язык осмысленным и полезным способом. Исследования показывают, что методы NLP используются правоохранительными органами и полицейскими департаментами в различных видах деятельности. К ним относятся административная практика, судебные расследования, анализ данных о преступлениях, преобразование речи в текст для отчетности и документирование преступной деятельности. Огромный объем текстовых данных — от стенограмм интервью, заявлений свидетелей, онлайн-сообщений и сообщений в социальных сетях, извлеченных в рамках уголовных расследований, — можно быстро и эффективно проанализировать с помощью NLP. Эта эффективность особенно важна, когда требуется быстрое понимание ситуаций в реальном времени, таких как похищения или захваты заложников, во время или после террористических атак и при расследовании случаев жестокого обращения с детьми.

Основные задачи, выполняемые NLP в полиции:

— *классификация текста:* аналитик, обрабатывающий текстовые данные, часто помечает преступления ключевыми словами, чтобы помочь понять обстоятельства, окружающие конкретное правонарушение, например, находился ли преступник под воздействием алкоголя или наркотиков. Поскольку преступность постоянно развивается, эти метки могут быть неполными. Одним из примеров классификации текста является назначение различных меток для подгрупп отмывания денег;

— *кластеризация:* в отличие от текстовой аналитики, которая опирается на предопределенные характеристики, кластеризация может помочь сгруппировать похожие преступления. Кластеризация отображает тексты в многомерное пространство, так что похожие тексты находятся близко друг к другу. В этой задаче не требуются метки. Кроме того, кластеризация может учитывать такие факторы, как время и местоположение, чтобы обеспечить целостное представление о тенденциях преступности. Например, в сценариях взлома кластеризация может выявить новые методы, такие как подвешивание ключей через почтовые ящики или использование определенных слабых мест замков;

— *резюмирование текста:* это метод, используемый для создания краткого и точного резюме длинных текстов, сохраняющего общий смысл. В области обработки естественного языка используются два основных подхода: на основе извлечения и на основе абстракции. Резюмирование на основе извлечения включает в себя извлечение подмножества слов или предложений, которые инкапсулируют ключевые моменты из текста, что может привести к грамматическим неточностям. Резюмирование на основе абстракции использует передовые методы глубокого обучения для перефразирования и сжатия исходного документа, аналогично человеческому резюмированию. Создавая новые фразы и предложения, которые инкапсулируют важную информацию из исходного текста, абстрактные алгоритмы машинного обучения оказывают ценную помощь в устранении грамматических ограничений, связанных с методами, основанными на извлечении. Эта технология играет важную роль в оказании помощи правоохранитель-

ным органам в их работе по анализу обширных полицейских отчетов и другой информации. Эта технология может предоставить правоохранительным органам краткие резюме, которые охватывают важные детали, не жертвуя точностью;

— *машинный перевод:* системы автоматизированного перевода облегчают преобразование текста с одного языка на другой. Эти модели принимают текст на указанном исходном языке в качестве входных данных и выдают соответствующий текст на указанном целевом языке в качестве выходных данных. Google Translate выделяется как хорошо известный пример такого основного приложения. Системы машинного перевода играют жизненно важную роль в правоохранительной деятельности, обеспечивая эффективный анализ многоязычных коммуникационных данных. Эти системы ускоряют обработку больших объемов информации, помогая следователям раскрывать потенциальные угрозы и выявлять преступную деятельность, преодолевая языковые барьеры. Технология улучшает глобальное сотрудничество между правоохранительными органами, обеспечивая более плавную коммуникацию и обмен информацией во время международных расследований. Кроме того, автоматизированный перевод способствует сбору доказательств, точно переводя различные формы доказательств, тем самым уменьшая языковую предвзятость.

Реальные приложения NLP в работе полиции разнообразны и постоянно развиваются. В подразделениях по борьбе с киберпреступностью NLP помогает анализировать преступную коммуникацию, расшифровывать скрытые значения или отмечать потенциально опасный онлайн-контент. Например, основными проблемами в борьбе с киберпреступностью являются обнаружение хищнических коммуникаций, идентификация интернет-преступников и предотвращение жестокого обращения с детьми и онлайн-груминга.

Обработка естественного языка может стать переломным моментом для работы полиции в этом отношении. Подзадача NLP, распознавание именованных объектов (англ. named-entity recongnition, NER), помогает аналитикам маркировать объекты (сущности) в отчетах о преступлениях в соответствии с их типом, например лица, организации и транспортные средства. Это позволяет проводить более тонкую группировку и анализ преступлений: например, в контексте краж со взломом различать методы проникновения, такие как разбивание окна или взлом определенного типа замка. Кроме того, при просеивании огромных баз данных неструктурированного текста инструменты NLP могут извлекать важную информацию (извлечение сущностей), позволяя

полиции быстро и эффективно реагировать на критические ситуации, такие как угрозы жизни.

По сути, NLP выступает в качестве моста между сильно зависящей от контекста человеческой коммуникацией и эффективностью вычислительного анализа, снабжая правоохранительные органы мощным инструментом в их цифровом арсенале.

Цифровая криминалистика. Цифровая криминалистика превратилась в важнейшую дисциплину в сфере правоохранительной деятельности в условиях становящегося все более цифровизированным мира.

При хранении, передаче и обработке в цифровом виде огромных объемов информации способность точно исследовать цифровой след преступников имеет решающее значение для полиции. Искусственный интеллект обеспечивает расширенные возможности просеивания огромных хранилищ данных, автоматизируя процессы, которые традиционно занимают у экспертов-людей длительное время, позволяет быстро классифицировать, фильтровать и выделять соответствующую информацию на основе предопределенных критериев или шаблонов (например, классификация изображений или значения хеш-функции).

Разработано несколько инструментов и методов восстановления и анализа данных с использованием компонентов ИИ. Эти инструменты могут восстанавливать удаленные файлы, получать доступ к данным с поврежденных устройств и восстанавливать фрагменты информации в согласованные форматы. Эффективность этих инструментов заключается в их способности адаптироваться и учиться на каждом конкретном случае, повышая точность с течением времени.

Значительной проблемой в цифровом пространстве является обнаружение киберпреступности. Вредоносные действия, от взлома до попыток фишинга, часто оставляют едва заметные следы или маскируются в обычном веб-трафике; ИИ отлично справляется с выявлением закономерностей и аномалий в этих данных.

Постоянно обучаясь на основе новых данных, модели ИИ могут отличать обычный сетевой трафик от потенциальных угроз, даже если вредоносные действия развиваются или используют новую тактику.

Расшифровка данных — еще одна область, где ИИ показал себя многообещающим инструментом. Передовые методы шифрования могут стать серьезным препятствием для следователей. В то время как традиционная расшифровка включает, например, поиск ключей шифрования, ИИ способен предсказывать потенциальные шаблоны

шифрования или ускорять процесс расшифровки, сужая возможные ключи шифрования на основе распознавания образов.

Наконец, анализ цифровых следов на устройствах и платформах приобрел первостепенное значение, особенно с распространением взаимосвязанных устройств в Интернете вещей. Один человек может ежедневно взаимодействовать с несколькими устройствами, от смартфонов и ноутбуков до устройств умного дома. Искусственный интеллект может отслеживать эти взаимодействия, создавая всеобъемлющий цифровой профиль, который помогает исследователям понять связи субъекта, или даже предлагать дополнительные элементы для дальнейшего анализа.

Цифровая криминалистика, усиленная возможностями ИИ, преобразила следственный ландшафт, предлагая беспрецедентную глубину и скорость анализа цифровых данных. Это не только повышает эффективность расследований, но и позволяет правоохранительным органам активно бороться с развивающимися цифровыми угрозами.

Компьютерное зрение и биометрия. В быстро меняющемся ландшафте появление компьютерного зрения и биометрии стало переломным моментом для правоохранительных органов как с точки зрения профилактики, так и с точки зрения расследования. Поскольку города и сообщества сталкиваются с всплеском количества цифровых изображений из таких источников, как камеры видеонаблюдения, персональные устройства, крайне важно эффективно использовать эти обширные визуальные данные. В сочетании с биометрическими методами, которые используют уникальные физиологические особенности людей, эти технологии обещают новый рубеж в работе полиции. Слияние биометрии и ИИ может обеспечить сочетание эффективности и точности, предлагая глубокие знания для быстрого выявления преступников и в то же время защищая конфиденциальность людей, не имеющих отношения к делу. Поскольку правоохранительные органы ориентируются в вызовах и возможностях цифровой эпохи, компьютерное зрение и биометрия выделяются как бесценные союзники.

Видеомониторинг и анализ. Развитие технологий визуализации в сочетании с ИИ преобразило сферу деятельности правоохранительных органов. Некоторые из потенциально полезных приложений для правоохранительных органов включают:

— *обработку в реальном времени и обнаружение аномалий:* видеонаблюдение вышло за рамки пассивного наблюдения. Благодаря интеграции алгоритмов на основе ИИ видеопотоки можно обрабатывать в реальном времени, сканируя на наличие предопределенных шаблонов или аномалий. Эта возможность особенно актуальна в зонах с повышенными требованиями к безопасности. Система может оперативно уведомлять сотрудников службы безопасности о подозрительных действиях, таких как присутствие транспортных средств вблизи важных мест, оставленные без присмотра объекты, забытая сумка на транзитном узле или несанкционированные въезды. Кроме того, эта обработка в реальном времени может играть важную роль в управлении дорожным движением, мгновенно обнаруживая аварии или сбои, способствуя немедленному и обоснованному реагированию;

— *безопасность и управление мероприятиями:* для таких мероприятий, как публичные празднества, концерты или фестивали, безопасность и благополучие участников имеют первостепенное значение. Обеспечение безопасности этих мероприятий принципиально отличается от повседневной работы полиции. Проведенный вместо традиционных визуальных обзоров видеоанализ с использованием ИИ может предоставить подробную информацию об общем потоке участников. Это позволяет на ранней стадии обнаруживать потенциальные уязвимости и помогает в проактивном планировании. Кроме того, система способна определять ситуации, которые могут потребовать внимания, гарантируя, что все смогут спокойно насладиться мероприятием;

— *автоматическое сообщение об инцидентах:* одной из функций, которые привносит интеграция ИИ в видеоаналитику, является способность автономно сообщать об инцидентах. Если обнаруживаются предопределенные условия или сценарии, такие как общественные беспорядки или потенциальные угрозы безопасности, система ИИ может автоматически генерировать подробные отчеты об инцидентах и (или) отправлять оповещения сотрудникам для оценки ситуации. Это не только ускоряет процесс документирования, но и гарантирует, что даже незначительные инциденты, которые могут быть упущены из виду при ручном мониторинге, будут точно зафиксированы и устранены.

По сути, современный видеомониторинг и анализ расширяют возможности правоохранительных органов. Полицейские не просто наблюдают — они активно понимают и интерпретируют огромные объемы визуальных данных, имеющихся в их распоряжении. От улучшения управления дорожным движением в реальном времени до обеспечения общественной безопасности на масштабных мероприятиях — видеоаналитика на основе ИИ представляет собой преобразующий скачок в возможностях правоохранительных органов, предлагая беспрецедентную скорость и точность в обнаружении и реагировании на

инциденты, тем самым способствуя созданию более безопасной среды для всех.

Классификация изображений. В сфере компьютерного зрения классификация изображений все чаще становится критически важной областью. Инструменты ИИ, обученные категоризировать изображения на основе доминирующего контента или объектов, которые они обнаруживают, помогают правоохранительным органам, перегруженным изображениями, быстро и эффективно анализировать эти данные. Классификация изображений помогает быстро сортировать такие данные по группам на «подозрительные» и «неподозрительные» и даже организовать их по различным темам, событиям или временным рамкам. Этот оптимизированный подход значительно ускоряет следственные процессы.

Эволюция современных инструментов классификации изображений, особенно тех, которые работают на основе алгоритмов машинного обучения, позволила быстро обрабатывать огромные объемы данных. Такие инструменты не только разделяют изображения с минимальным ручным вмешательством, но и гарантируют, что ни одно важное визуальное доказательство не останется незамеченным. Кроме того, присущий этим системам уровень проверки обеспечивает точную категоризацию, что приводит к более эффективным результатам расследования. Помимо традиционных приложений, классификация изображений актуальна в различных областях правоохранительной деятельности. Например, во время публичных мероприятий или в местах массового скопления людей классификация изображений может выявить потенциальные угрозы или нарушения, помогая правоохранительным органам принимать превентивные меры.

Примечательным сценарием, который подчеркивает потенциал классификации изображений, является ее применение в расследованиях, анализе данных, извлеченных из мобильных коммуникационных устройств. Зачастую эти устройства хранят тысячи изображений, что делает навигацию по ним сложной и трудоемкой. Кроме того, эта ситуация вызывает серьезные опасения относительно защиты данных при обработке личных фотографий.

Благодаря классификации изображений с помощью ИИ изображения, извлеченные криминалистическим путем с мобильных устройств, могут быть быстро отсортированы, что сводит к минимуму необходимость ручного просмотра и объем обрабатываемых персональных данных. Сосредоточившись на соответствующих изображениях, следователи могут не только сэкономить драгоценное время, но и раскрыть важную информацию, которая могла бы быть упущена из виду в огромных объемах данных. По сути, классификация изображений формирует будущее цифровых расследований в правоохранительных органах, предлагая сочетание скорости, точности и эффективности.

Улучшение распределения ресурсов и стратегического планирования. Все более сложная картина правоохранительной деятельности требует стратегического подхода к распределению ресурсов. По мере развития угроз и расширения городов обеспечение оптимального использования ресурсов — будь то персонал, оборудование или время — становится обязательным.

Распределение ресурсов на основе ИИ. Искусственный интеллект обладает потенциалом для преобразования распределения ресурсов из реактивного подхода в проактивный, стратегический. Правоохранительные органы часто работают в условиях ограниченного бюджета и ограничений по персоналу. Тем не менее от них ожидают обеспечения безопасности расширяющихся городских пространств и устранения возникающих угроз. Обеспечение оптимального использования каждого ресурса — это не только вопрос эффективности, это критически важный для общественной безопасности и доверия фактор.

Стратегическое планирование на основе ИИ. Помимо ежедневного планирования ИИ играет роль в долгосрочном стратегическом планировании. Например:

— *организация патрулирования:* вместо стандартных маршрутов ИИ может разрабатывать маршруты патрулирования, которые меняются в зависимости от времени суток, дня недели или известных схем активности, гарантируя, что сотрудники полиции будут находиться там, где они, скорее всего, понадобятся.

Реагирование на чрезвычайные ситуации: ИИ может помочь в планировании быстрого реагирования на чрезвычайные ситуации, предлагая оптимальные маршруты, анализируя данные о дорожном движении в реальном времени или даже прогнозируя потенциальные вторичные инциденты или угрозы;

— *безопасность публичных мероприятий:* при проведении крупных публичных собраний, от концертов до спортивных мероприятий или парадов, могут возникать проблемы безопасности. Искусственный интеллект способен анализировать прошедшие события, динамику толпы, узкие места на входе/выходе и даже сообщения в социальных сетях, чтобы помочь разработать комплексный план безопасности;

— *оценка эффективности стратегий:* ИИ не просто предлагает инструменты для планирования, он также имеет решающее значение для оценки. Обзоры после инцидента могут быть проанализированы для определения эффективности развертываний или антикриминальной политики в целом. Были ли сотрудники полиции оптимально размещены? Соответствовали ли результаты анализа ИИ фактическим образцам? Такие оценки могут быть возвращены в систему, обеспечивая непрерывное обучение и пересмотр политик/стратегий.

Таким образом, распределение ресурсов и стратегическое планирование на основе ИИ повышают способность правоохранительных органов защищать сообщества. Превращая огромные объемы данных в действенные идеи и постоянно извлекая уроки как из успехов, так и из неудач, ИИ обеспечивает способность правоохранительных органов оставаться гибкими, проактивными и всегда адаптируемыми к меняющимся вызовам современного мира.

Технологические ограничения и проблемы. Несмотря на преимущества для правоохранительных органов, внедрение ИИ сталкивается с рядом технических ограничений, которые ставят под сомнение его эффективность и результативность:

— *качество и доступность данных* имеют основополагающее значение для эффективности ИИ в правоохранительной деятельности, но проблемы возникают из-за различий в методах сбора и хранения данных в разных юрисдикциях. Эти различия приводят к непоследовательным наборам данных, которые могут быть неполными или предвзятыми, что ставит под угрозу целостность результатов анализа ИИ. Кроме того, существующие данные часто не имеют необходимой детализации для приложений ИИ, поскольку изначально они собирались без учета его использования. Например, отчеты полиции, хотя и информативны, могут не охватывать незарегистрированные или необнаруженные инциденты, искажая процесс обучения ИИ и его результаты. Стандартизированные методы сбора информации вместе с очисткой и обогащением данных необходимы для получения полных и объективных информационных массивов. Кроме того, интеграция надежных методов защиты данных крайне важна для сохранения конфиденциальности пользователей и соблюдения актуальных правил информационной безопасности.

Решив эти проблемы, можно повысить надежность использования ИИ в работе правоохранительных органов, и тогда он будет лучше отражать и решать задачи борьбы с преступной деятельностью, соблюдая при этом этические и правовые стандарты;

— *проблемы интеграции:* при интеграции ИИ с существующими системами правоохранительных органов и конвейерами обработки данных возникают различные технические препятствия. Несовместимость современных решений ИИ и старых технологических инфраструктур может привести к значительным проблемам интеграции, влияющим на обмен данными и эффективность работы. Для устранения этого разрыва требуется двойной подход: модернизация устаревших систем для повышения их совместимости с технологиями ИИ и проектирование будущих решений ИИ с упором на совместимость и модульную интеграцию;

— *масштабируемость и производительность* в различных условиях: эффективность инструментов ИИ в правоохранительных органах должна поддерживаться независимо от масштаба данных или сложности операционных сценариев. Изменчивость инцидентов и условий окружающей среды проверяет на адаптивность системы ИИ. Решение этих проблем требует разработки моделей ИИ, которые не только масштабируемы, но и универсальны, способны адаптироваться к различным объемам данных и операционным требованиям без ущерба для производительности;

— *техническое обслуживание и техническая поддержка:* быстро развивающаяся природа технологии ИИ требует постоянных обновлений и обслуживания для обеспечения эффективности и безопасности. Однако необходимая постоянная техническая поддержка может истощить ресурсы правоохранительных органов, особенно тех, у кого ограниченный доступ к IT-экспертизе. Создание специализированных структур поддержки и использование партнерских отношений с поставщиками технологий может обеспечить устойчивые решения этих проблем, гарантируя, что системы ИИ будут оставаться актуальными и эффективными.

Задача не является простой и требует уточнения структуры управления ИИ и согласованных усилий множества заинтересованных сторон. Сотрудничество между правоохранительными органами, разработчиками технологий, политиками и сообществом имеет решающее значение для преодоления этих технологических ограничений. Благодаря такому сотрудничеству можно разрабатывать, тестировать и совершенствовать инновационные решения для повышения эффективности, надежности и общей результативности приложений ИИ в полицейской практике. Кроме того, инвестиции в исследования и разработки, сосредоточение внимания на этическом использовании ИИ и создание среды непрерывного обучения и адаптации среди сотруд-

ников правоохранительных органов являются ключевыми шагами на пути к преодолению этих препятствий.

§ 2. Использование правоохранительными органами генеративной модели искусственного интеллекта ChatGPT

Генеративный предварительно обученный преобразователь (англ. generative pre-trained transformer, GPT) — это чат-бот, языковая модель ИИ, основанная на типе нейронной сети, называемом трансформером, которая предназначена для обработки последовательных данных, таких как текст, способна производить письменный текст в различных формах (статьи, поэмы, эссе, речи и т. п.), используя образцы, собранные из Интернета.

Модель GPT является «предварительно обученной», что означает: она обучается на большом количестве текстовых данных, прежде чем будет адаптирована для конкретной задачи.

ChatGPT был разработан OpenAI, организацией по исследованию ИИ, и является одной из самых передовых языковых моделей, доступных в настоящее время.

В связи с доступностью и мощью ChatGPT, его способностью проникать в повседневную деятельность по сбору информации так же, как это делают поисковые системы, правоохранительные органы должны предвидеть использование подобных приложений преступниками. Цель этого параграфа — предоставить обзор функциональных возможностей и ограничений ChatGPT, а также дать рекомендации по его применению для правоохранительных органов.

ChatGPT научили понимать шаблоны и структуры языка и генерировать новый текст, похожий по стилю и тону. ChatGPT — это интерактивный интерфейс ИИ, способный участвовать в разговорах, отвечая на последующие вопросы, распознавая собственные ошибки, подвергая сомнению несоответствия и отклоняя определенные запросы. Это система чат-ботов ИИ, способная «понимать естественный человеческий язык» и предоставлять информацию и решения для сложных вопросов.

Предназначение ИИ не только в анализе существующих данных, но и в создании совершенно нового контента. Генеративный ИИ — быстро развивающаяся область, использует алгоритмы для генерации контента, включающего не только тексты, но и изображения и другие формы медиа. Эти технологии изучают шаблоны, структуры и нюансы из огромных наборов данных, а затем производят новые данные, придерживаясь тех же шаблонов. Например, после анализа тысяч изображений кошек генеративная модель может создать новое, синтетическое изображение кошки, которое, хотя и является полностью вымышленным, выглядит неотличимо реальным. Наиболее известные формы генеративного ИИ — генеративные состязательные сети (GAN) и большие языковые модели (LLM).

Генеративно-состязательные сети (англ. generative adversarial Network, GAN) — это класс фреймворков машинного обучения, в которых одна нейронная сеть учится генерировать максимально реалистичные синтетические данные, а другая нейронная сеть учится обнаруживать синтетические данные. В то время как сети взаимодействуют друг с другом, обе непрерывно улучшают свою производительность. Сети, генерирующие синтетические данные, широко используются в генерации изображений, видео и все чаще в других областях, таких как музыка.

Они могли бы предложить правоохранительным органам способы оценки производительности биометрических систем без ущерба для конфиденциальности личности. Например, GAN могут помочь генерировать синтетические изображения лица, отпечатки пальцев и другие биометрические данные, которые, в свою очередь, могут использоваться вместо реальных данных, когда реальные данные недоступны, для оценки точности и надежности систем распознавания в различных группах населения и условиях. Кроме того, они позволяют разрабатывать технологии антиспуфинга для борьбы с мошенничеством с идентификацией. Однако по мере принятия этих технологий правоохранительным органам крайне важно сбалансировать преимущества с этическими соображениями и защитой конфиденциальности, гарантируя, что использование синтетических носителей поддерживает общественную безопасность при соблюдении прав личности.

Большие языковые модели (LLM) относятся к форме генеративного ИИ с приложениями в обработке естественного языка (NLP). Эти модели предназначены для обработки и генерации человеческого языка. Обучаясь на обширных текстовых наборах данных, они способны выполнять различные языковые задачи. Эти модели знаменуют собой существенный прогресс в том, как машины понимают и воспроизводят человеческий язык, с широкими последствиями для множества секторов, таких как технологии, развлечения, образование и т. д.

К преимуществам, которые LLM могут предложить правоохранительным органам, относятся поддержка следователей в расследовании незнакомых областей преступности, содействие исследованию откры-

тых источников и анализу разведданных, а также разработка технических следственных инструментов. Кроме того, LLM могут ускорить выполнение многочисленных административных задач, таких как написание отчетов и обобщение информации. Тем не менее использование LLM правоохранительными органами потребует безопасной среды, которой можно доверять конфиденциальную информацию, а также тщательных оценок, касающихся защиты основных прав и смягчения потенциального предубеждения.

Несмотря на впечатляющие способности, LLM имеют ряд ограничений, таких как склонность производить фактически неточный или нелогичный контент, обычно называемый галлюцинациями. Дополненная поиском генерация (англ. retrieval-augmented generation, RAG) появляется как потенциальное решение некоторых из этих проблем. В то время как многие LLM в первую очередь полагаются на уже существующие знания или общедоступную информацию для создания текста, RAG идет на шаг дальше, интегрируя механизмы поиска информации. Это означает, что модели RAG могут активно искать и включать соответствующую информацию из заранее определенных авторитетных источников знаний, гарантируя, что сгенерированный контент будет не только связным, но и контекстуально точным и актуальным. Таким образом, организации имеют большее влияние на производимый текстовый контент, в то время как пользователи лучше понимают процесс, посредством которого LLM генерирует свой ответ.

Изучение возможностей RAG в обработке наборов данных уголовных расследований имеет важное значение, однако к этому следует подходить методично и в соответствии с нормативными требованиями. В нынешнюю эпоху, когда информация имеет первостепенное значение, существует беспрецедентный спрос на инновационные методы для изучения и интерпретации сложных данных.

Генеративный ИИ представляет собой следующий скачок, переход от пассивного анализа к активному творчеству. Для правоохранительных органов он предлагает кладезь возможностей. Однако его сила заключается в его разумном и этическом применении, балансирующем между инновациями и ответственностью.

Использование ChatGPT правоохранительными органами. Платформа OpenAI универсальна, но ее обычное использование включает поиск, создание и изменение изображений, написание контента, такого как поэмы, песни, эссе и даже блоги, а также отладку кода или принуждение Codex написать его. В целом, модель GPT представляет собой крупный прорыв в разработке языковых моделей ИИ. Ее различные версии раздвинули границы и открыли новые возможности для инноваций и открытий.

ChatGPT следует использовать с учетом соответствующих законов, правил, внутренней политики и процедур каждого правоохранительного и судебного органа. В дополнение к национальным законам — и особенно при отсутствии конкретных законов в области ИИ — все виды использования ChatGPT должны соответствовать международным стандартам ответственного ИИ, следует придерживаться таких принципов, как законность, минимизация вреда, справедливость, уважение человеческой автономии и надлежащее управление.

ChatGPT никогда не должен заменять человеческое суждение, и окончательная ответственность за точность и качество выходных данных ChatGPT и принятых решений должна лежать на отдельных сотрудниках правоохранительных органов, которые имеют необходимую подготовку и опыт.

Ниже приведены некоторые потенциальные варианты использования ChatGPT для правоохранительных органов. Однако это чисто гипотетические сценарии, требующие индивидуальной оценки и мер безопасности, которые должны быть реализованы правоохранительными и судебными органами:

— *перевод:* ChatGPT можно использовать для перевода текста с одного языка на другой. Это может быть полезно в ситуациях, когда языковой барьер составляет проблему. Однако на ChatGPT не следует полагаться без подтверждения и проверки вывода, особенно в отношении переводов, которые будут использоваться для возбуждения дела, принятия мер против лица, обработки свидетельских показаний или обработки конфиденциальной информации;

— *анализ текстовых данных:* правоохранительные органы часто имеют дело с большими объемами текстовых данных, такими как электронные письма, сообщения в социальных сетях и стенограммы чатов. ChatGPT можно использовать для анализа этих данных и извлечения информации, которая может иметь отношение к текущим расследованиям;

— *обнаружение мошенничества:* ChatGPT можно использовать для анализа текстовых данных и выявления схем мошенничества или другой преступной деятельности, такой как фишинговые атаки или мошеннические электронные письма;

— *обучение и образование:* ChatGPT можно использовать для обучения и образования сотрудников правоохранительных органов по та-

ким темам, как методы деэскалации, понимание культурных различий и методы расследования;

— *поддержка жертв:* ChatGPT можно использовать для предоставления поддержки и ресурсов жертвам преступлений, например информации о законных правах и консультационных услуг;

— *расследования:* ChatGPT можно использовать для проведения следственных действий, таких как анализ интернет-форумов или групп в социальных сетях для выявления потенциальных подозреваемых или преступной деятельности;

— *виртуальные помощники:* ChatGPT может использоваться для предоставления виртуальных помощников, которые используют методы обработки естественного языка для понимания и ответа на запросы пользователей.

Важно отметить, что необходимо проявлять особую осторожность, чтобы гарантировать, что использование ИИ не приведет к предвзятости или нарушению прав личности и конфиденциальности. При использовании ChatGPT в целях обеспечения соблюдения закона правоохранительные органы должны проявлять осторожность в отношении потенциальных проблем конфиденциальности и раскрытия данных.

Платформы ИИ, такие как ChatGPT, не следует использовать для размещения конфиденциальных данных полиции, поскольку их поставщики могут обрабатывать эту информацию на своих серверах в учебных целях. Кроме того, вполне вероятно, что при использовании ChatGPT по уголовному делу на основе данных правоохранительных органов будут приниматься судебные решения с требованием разъяснить запрос, сделанный ChatGPT правоохранительными органами.

Ограничения ChatGPT. Большая языковая модель ИИ, такая как ChatGPT, может иметь несколько ограничений, которые способны повлиять на качество и точность ее ответов. Эти ограничения важно учитывать при использовании ChatGPT в качестве инструмента для генерации ответов на текстовые запросы, особенно в контексте правоохранительных органов:

— *неполная или устаревшая информация:* хотя ChatGPT был обучен на большом наборе текстовых данных, его производительность в значительной степени зависит от качества и релевантности его обучающих данных. Недостаточные или низкокачественные данные могут привести к плохой производительности и неточным ответам. Это означает, что у него может быть недостаточно знаний или понимания, чтобы предоставить точные или полные ответы на некоторые вопросы, особенно по очень специфическим или редким темам. Более

того, ChatGPT может не знать о последних событиях, обновлениях или достижениях в различных областях в зависимости от даты окончания получения обучающих данных, что также может привести к устаревшей информации;

— *предвзятость:* как любая модель машинного обучения, ChatGPT также может быть предвзятым в отношении определенных групп, тем или точек зрения в зависимости от данных обучения. Данные обучения ChatGPT получены из широкого спектра источников, включая социальные сети, новостные статьи и книги. Это означает, что модель может содержать предвзятость из этих источников, например, по признаку пола, расы или культуры, что может потенциально привести к неточным или дискриминационным ответам. Иногда она может генерировать ответы, которые непреднамеренно оскорбительны или неуместны;

— *понимание контекста:* ChatGPT иногда может испытывать трудности с пониманием нюансов и контекста вопроса или разговора, что может привести к нерелевантным или неуместным ответам;

— *уязвимость к состязательным атакам:* ChatGPT может быть уязвим к атакам, во время которых злоумышленники намеренно вводят неверную или вводящую в заблуждение информацию, чтобы манипулировать ответами модели;

— *отсутствие юридической экспертизы:* хотя ChatGPT обучается на разнообразном контенте, он не является экспертом по праву. Его понимание юридических концепций, терминологии и процедур может быть неполным или неверным, поэтому на него не следует полагаться для профессиональной юридической консультации.

Осведомленность и осторожность. Генеративный ИИ и большие языковые модели, такие как ChatGPT, имеют много потенциальных преимуществ. Однако важно знать о возможных злоупотреблениях, сохранять бдительность, выявлять потенциальные уязвимости и принимать превентивные меры. Поскольку область генеративного ИИ все еще не регулируется (с незначительной модерацией или без нее), она создает новую питательную среду для расширения существующих и возникновения будущих преступных предприятий.

Искусственный интеллект становится все более доступным и будет и далее распространяться в киберпреступности. Правоохранительным органам необходимо иметь инструменты, способные обнаруживать ChatGPT или контент, сгенерированный ИИ, и иметь возможность делиться этими инструментами и, возможно, подписью идентифициро-

ванного контента, сгенерированного ИИ. Разрабатывается ряд таких инструментов для обнаружения текста, сгенерированного ИИ.

Правоохранительные органы должны быть хорошо подготовлены и гарантировать, что ChatGPT и аналогичные платформы используются для общего блага, выявлять любое их преступное использование.

Важно внедрить механизм для получения, обмена и распространения информации среди правоохранительных органов, который должен включать:

— *согласование технологий:* для платформ, использующих ИИ и связанные с ним процессы, важно, чтобы следователи правоохранительных органов, специалисты по судебной экспертизе и прокуроры обладали необходимым уровнем знаний и навыков, чтобы гарантировать, что эти технологии будут применяться надлежащим образом в ходе расследований;

— *стандартные следственные процессы и процедуры:* важно, чтобы правоохранительные органы работали с разработчиками над созданием стандартных процессов и процедур для борьбы с транснациональной преступностью. Четкое понимание общих потребностей правоохранительных органов и партнеров отрасли и взаимные решения имеют важное значение;

— *стандартизированное обучение и образование:* существует огромный интерес к платформам разговорного ИИ, связанным с ними технологиям и процессам из-за их расширенных функциональных возможностей. Поэтому жизненно важно выделять ресурсы и оказывать поддержку для создания учебных и образовательных пакетов.

§ 3. Модель искусственного интеллекта DeepSeek и ее значение для предупреждения преступлений

Новая модель ИИ от китайского стартапа DeepSeek привлекла внимание всего мира своими передовыми возможностями рассуждений и экономичным методом обучения. Хотя ее производительность соперничает с другими современными моделями, такими как OpenAI, оценка безопасности выявила критические недостатки в этой сфере.

Почему эта модель так важна? Современные модели ИИ требуют вложения сотен миллионов (и даже миллиардов) долларов и огромных вычислительных ресурсов для создания и обучения, несмотря на достижения последних лет в эффективности затрат и вычислений. С помощью своих моделей DeepSeek показала сопоставимые с ведущими

передовыми моделями результаты, потребляя при этом значительно меньше ресурсов.

DeepSeek R1-Zero (обученный исключительно с помощью обучения с подкреплением) и DeepSeek R1 (уточнение R1-Zero с помощью контролируемого обучения) демонстрируют сильный акцент на разработке LLM с расширенными возможностями рассуждения. Модели DeepSeek сопоставимы с моделями OpenAI o1, при этом превосходят Claude 3.5 Sonnet и ChatGPT-4o в таких задачах, как математика, кодирование и научное рассуждение.

Разницу в обучении моделей DeepSeek можно обобщить тремя следующими принципами:

1) цепочка мыслей позволяет модели самостоятельно оценивать свою эффективность;

2) обучение с подкреплением помогает модели управлять собой;

3) дистилляция позволяет разрабатывать меньшие модели (от 1,5 млрд до 70 млрд параметров) из исходной большой модели (671 млрд параметров) для более широкой доступности.

Подсказки *цепочки мыслей* позволяют моделям ИИ разбивать сложные проблемы на более мелкие шаги, подобно тому, как люди показывают свою работу при решении математических задач. Этот подход сочетается с «заполнением черновиков», когда модели могут работать с промежуточными вычислениями отдельно от своего окончательного ответа. Если модель совершает ошибку в ходе этого процесса, она может вернуться к более раннему правильному шагу и попробовать другой подход.

Кроме того, методы *обучения с подкреплением* вознаграждают модели за создание точных промежуточных шагов, а не только правильных окончательных ответов. Эти методы значительно улучшили производительность ИИ в сложных задачах, требующих детального обоснования.

Дистилляция — это метод создания меньших эффективных моделей, которые сохраняют большинство возможностей больших моделей. Он работает с использованием большой модели «учителя» для обучения меньшей модели «ученика». Благодаря этому процессу модель DeepSeek учится решать проблемы для определенных задач, требуя при этом меньше вычислительных ресурсов.

DeepSeek объединил цепочку подсказок и моделирование вознаграждения с дистилляцией для создания моделей, которые значительно превосходят традиционные большие языковые модели в задачах рассуждения, сохраняя при этом высокую операционную эффективность.

Уязвимости DeepSeek. Парадигма DeepSeek новая. Если ранее поставщики сосредоточивались на построении моделей с рассуждениями, выполняющих задачи адаптивным образом посредством непрерывного взаимодействия с пользователем, то команда DeepSeek продемонстрировала высокую производительность, не полагаясь на дорогие, маркированные человеком наборы данных или огромные вычислительные ресурсы.

Нет сомнений, что производительность модели DeepSeek оказала огромное влияние на ландшафт ИИ. Однако нельзя сосредоточиваться исключительно на производительности, необходимо понять, есть ли у DeepSeek и его новой парадигмы рассуждений какие-либо существенные компромиссы, когда дело касается безопасности.

Так, было проведено тестирование безопасности и надежности с использованием нескольких популярных пограничных моделей, а также двух моделей рассуждений: DeepSeek R1 и OpenAI o1-preview. Для оценки этих моделей был запущен автоматический алгоритм джейлбрейка[1] на 50 однородно отобранных подсказках из популярного бенчмарка HarmBench. Бенчмарк HarmBench — стандартизированная система оценки методов выявления рисков злонамеренного использования LLM — имеет в общей сложности 400 вариантов поведения в 7 категориях вреда, включая киберпреступность, дезинформацию, незаконную деятельность и общий вред.

Ключевая метрика — показатель успешности атак (ASR). Были использованы как автоматические методы обнаружения отказов, так и человеческий контроль для проверки джейлбрейков.

Исследовательская группа сумела взломать DeepSeek R1 со 100%-ным показателем успешности атаки. Это означает, что не было ни одного запроса из набора HarmBench, который не получил бы утвердительного ответа от DeepSeek R1. Это контрастирует с другими пограничными моделями, например с o1 от OpenAI, которая блокирует большинство состязательных атак с помощью своих модельных защитных ограждений.

Фишинговые атаки DeepSeek с использованием ИИ. Подобно ChatGPT и другим платформам генеративного ИИ, *выпуск DeepSeek позволит киберпреступникам создавать сложные атаки в масштабе.* И если история повторится, вероятно, эти атаки усилятся в ближайшие недели, поскольку злоумышленники используют новую доступ-

[1] Джейлбрейк (англ. jailbreak — побег из тюрьмы, взлом) — снятие программных ограничений, наложенных производителем на устройство, для обеспечения их свободного изменения, взлом программы.

ную технологию в своих интересах. Но что отличает DeepSeek от других платформ генеративного ИИ?

Во-первых, DeepSeek предположительно был обучен командой из Китая с относительно небольшими вычислительными ресурсами. Модели такого качества до сих пор появлялись только в очень хорошо финансируемых исследовательских лабораториях (таких как OpenAI). Поэтому следует ожидать, что в будущем мы увидим более мощные модели от менее обеспеченных ресурсами групп.

Во-вторых, DeepSeek — это модель с открытым исходным кодом (как серия Llama от Meta[1]), что означает: любой человек в любой точке мира может загрузить модель, изменить ее по своему желанию и запустить на своей собственной инфраструктуре. В отличие от инструментов вроде ChatGPT, у которых есть компания (OpenAI), теоретически ответственная за то, чтобы люди не использовали инструмент в злонамеренных целях, модели с открытым исходным кодом могут использоваться киберпреступниками без каких-либо ограничений.

Риски кибербезопасности, связанные с искусственным интеллектом DeepSeek. Поскольку модели DeepSeek AI получают всемирную популярность, они могут вызвать серьезные проблемы безопасности, особенно когда речь идет о социальной инженерии. Эти языковые модели способны легко составить убедительную фишинговую или компроматную атаку на деловую электронную почту (BEC) с правильной грамматикой и конкретными призывами к действию, что еще больше усложняет для людей возможность отличить безопасное общение от вредоносного.

К сожалению, инструменты вроде DeepSeek становятся все более доступными и злоумышленники могут использовать ИИ для создания *гиперперсонализированных фишинговых атак* в реальном времени в беспрецедентных масштабах.

DeepSeek и другие генеративные модели ИИ. Ключевыми отличиями DeepSeek AI являются его невысокая стоимость и высокая производительность. Более низкий барьер для входа означает, что киберпреступники могут использовать DeepSeek AI для генерации фишингового контента в больших масштабах без значительных инвестиций.

Кроме того, в отличие от моделей OpenAI, которые размещаются в контролируемых средах с ограничениями доступа на основе API, DeepSeek AI является моделью с открытым исходным кодом. Это означает, что ее можно свободно загружать, изменять и развертывать в

[1] Компания Meta признана экстремистской организацией и запрещена в Российской Федерации.

частной инфраструктуре, устраняя механизмы надзора, предназначенные для предотвращения злоупотреблений. Таким образом, субъекты угроз могут манипулировать моделью, чтобы обойти средства контроля безопасности, что значительно усложняет обнаружение и смягчение последствий.

Борьба с ИИ с помощью ИИ: поведенческий подход Abnormal к нейтрализации угроз ИИ DeepSeek. Причина, по которой атаки с использованием ИИ, включая атаки DeepSeek AI, продолжают достигать конечных пользователей, заключается в том, что устаревшие системы не были настроены на защиту от них. Сигнатуры, на которые полагаются безопасные шлюзы электронной почты, защищающие внутренний почтовый сервер (SEG), чтобы предотвратить атаки, не справляются с фишингом на основе текста, управляемым ИИ. Кроме того, SEG, требующие постоянного обновления правил, будут постоянно пропускать адаптивные атаки, которые разработаны для их обхода. Защиту от сложных киберугроз (фишинг, BEC, ATO и др.) обеспечивает платформа на базе ИИ — Abnormal.

В Abnormal разработаны системы обнаружения кибератак, чтобы быть устойчивыми к этим видам атак следующего поколения, поддерживаемых ИИ.

Ключевые компоненты платформы Abnormal AI, которые позволяют обнаруживать атаки — независимо от того, генерируются они людьми или ИИ, — включают:

— *поведенческий ИИ:* понимает закономерности общения внутри организации, чтобы выявлять едва заметные аномалии и обнаруживать ранее невиданные угрозы в режиме реального времени, даже при отсутствии вредоносных ссылок или вложений;

— *идентификацию и сбор информации о поставщиках:* отслеживает обычное поведение сотрудников и поставщиков, отмечая подозрительные отклонения в тоне, срочности и истории отправителя;

— *адаптивные механизмы защиты:* Abnormal постоянно обновляет свои модели обнаружения, поскольку злоумышленники находят новые способы использования ИИ для совершенствования своих атак.

Кроме того, *автоматизированный ответ Abnormal* позволяет платформе обнаруживать аномалии, указывающие на атаку, не давая конечным пользователям реагировать на нее, поэтому людям никогда не приходится принимать решение о том, является электронное письмо вредоносным или нет.

§ 4. Этические и социальные проблемы применения искусственного интеллекта в правоохранительных органах

Искусственный интеллект становится все более важным инструментом для поддержания правопорядка. Тем не менее это порождает множество этических и социальных проблем, требующих тщательного анализа.

Предвзятость и справедливость данных. Данные являются ядром любой системы ИИ, и качество данных напрямую влияет на результаты, выдаваемые системой. Любое искажение данных может непреднамеренно привести к несправедливым или предвзятым результатам. Справедливая и беспристрастная охрана правопорядка является основополагающим столпом демократических обществ, и поэтому распознавание и устранение предвзятости является предметом особой заботы правоохранительных органов.

Предвзятость данных может возникать из множества источников. Исторические данные, используемые для обучения систем ИИ, могут включать в себя давние общественные предубеждения, отражающие прошлые предрассудки и дискриминационные практики. Например, если определенный район исторически подвергался чрезмерному контролю из-за расовых или социально-экономических предубеждений, система ИИ, обученная на этих данных, может предположить, что этот район более подвержен преступной деятельности. Такие результаты могут создать обратную связь, заставляя правоохранительные органы продолжать чрезмерно контролировать этот район, тем самым обнаруживая непропорционально большое количество преступлений и усиливая предубеждения, присутствующие в данных.

Помимо исторических предубеждений, существует также проблема предвзятости репрезентации. Если данные не представляют адекватно все сегменты населения, система ИИ может делать ошибочные прогнозы.

Стоит отметить, что не существует универсального соглашения о точных определениях справедливости. Существуют различные толкования. В некоторых случаях оправдано использование защищенных категорий, таких как пол и возраст. Например, система ИИ, которая вычитает информацию о несовершеннолетних для обеспечения дополнительной защиты, должна быть обучена с использованием соответствующих конфиденциальных данных. Таким образом, эти ситуации следует оценивать индивидуально, и, в конечном итоге, люди всегда

должны определять, как действовать на основе информации, предоставленной ИИ.

Конфиденциальность и наблюдение. В правоохранительных органах поиск правильного баланса между общественной безопасностью и личной конфиденциальностью всегда был проблемой. По мере того, как ИИ все глубже интегрируется в методы полицейской деятельности, этот баланс становится еще более хрупким.

Хотя ИИ предлагает значительные преимущества для правоохранительных органов, такие как способность обрабатывать огромные объемы данных и использовать биометрию для быстрой идентификации преступников и оценки угроз, он также приносит с собой сложные проблемы. Передовые технологии, такие как системы распознавания лиц, могут значительно повысить эффективность. Однако без достаточных гарантий, таких как человеческий надзор для оценки их результатов, эти технологии рискуют нарушить основные права, такие как право на частную жизнь и право на личную жизнь. Это может проявляться в непропорциональном наблюдении за невиновными лицами или в возможности злоупотребления, направленного на определенные группы, что вызывает обеспокоенность по поводу конфиденциальности и необходимости такого мониторинга.

Подотчетность и прозрачность. Несмотря на преимущества, которые приносит технология, одной из главных проблем является возможность того, что решения, прогнозы или рекомендации, сделанные ИИ, останутся необъясненными или неоправданными. Когда выходные данные ИИ используются для поддержки принятия решений в правоохранительных органах — будь то биометрическая идентификация или оценка угроз — крайне важно, чтобы и сотрудники полиции, и те, кого затрагивают эти решения, понимали обоснование. Без этой ясности возрастает риск недоверия, злоупотреблений и потенциальной несправедливости.

Уникальная природа ИИ, где алгоритмы часто оперируют уровнями сложности, выходящими за рамки человеческого понимания, создает новые проблемы.

Существует острая необходимость в механизмах, которые сделают процессы принятия решений ИИ интерпретируемыми, особенно в таких ответственных сферах, как охрана правопорядка и уголовное правосудие, не только с точки зрения сбора, обработки и представления в суде или трибунале соответствующих доказательств, но и в более широком смысле, чтобы гарантировать, что граждане смогут понимать, взаимодействовать и оспаривать использование ИИ.

Обеспечение подотчетности также подразумевает установление четких обязанностей. Когда инструмент ИИ используется для генерации рекомендаций или прогнозирования, кто должен нести ответственность в случае ошибки или несправедливости? Разработчики программного обеспечения, правоохранительные органы, использующие инструмент, или всеобъемлющий регулирующий орган? Определение ответственности имеет жизненно важное значение для обеспечения того, чтобы инструменты ИИ в правоохранительных органах оставались эффективными и справедливыми.

Проблема черного ящика. В дискуссиях, касающихся прозрачности ИИ, центральным и насущным вопросом является загадочная проблема черного ящика. По своей сути дилемма черного ящика подчеркивает непрозрачность, присущую сложным алгоритмам ИИ, с особым акцентом на сложности моделей глубокого обучения. Эти модели машинного обучения разработаны для имитации обработки информации человеком. Используя несколько слоев искусственных нейронов, подключенных к сети, для извлечения расширенных функций из входных данных, они носят ярлык «глубокие». Однако глубокие вопросы вызывает их способность принимать решения или делать прогнозы, не имея четкого, линейного объяснения их обоснования. Подобно непрозрачному запечатанному черному ящику, эти алгоритмы выдают результаты, не раскрывая свою внутреннюю работу, чтобы можно было оценить применяемую логику.

В сфере охраны правопорядка эта непрозрачность представляет собой существенную проблему. Когда система, управляемая ИИ, высказывает опасения относительно потенциальной угрозы со стороны отдельного лица или рекомендует увеличить количество патрульных в определенном районе, для сотрудников правоохранительных органов и лиц, затронутых такими решениями, становится крайне важным понять лежащую в основе логику. Отсутствие этого критического понимания открывает дверь для потенциально неконтролируемых предубеждений, ошибок или неверных толкований, поднимаются фундаментальные вопросы ответственности и правосудия.

Разрешение проблемы черного ящика — это не только технический вопрос; это глубокий этический императив. Инновационные решения, такие как объяснимый ИИ (XAI), активно разрабатываются, чтобы преодолеть этот разрыв и сделать алгоритмы более прозрачными и понятными. Однако до тех пор, пока такие решения не станут общедоступными и стандартизированными, проблема черного ящика останется весьма острой в продолжающемся стремлении к основан-

ной на ИИ структуре полицейской деятельности, которая будет подотчетной, справедливой и прозрачной для всех заинтересованных сторон.

Также следует отметить, что алгоритмы ИИ могут быть непрозрачными из-за их защищенного статуса коммерческой тайны. В таких случаях подробности внутренней алгоритмической работы остаются закрытыми, чтобы защитить коммерческую тайну и избежать манипуляций с системой.

Права человека и дискриминация. Основной проблемой является непреднамеренное усиление общественных предубеждений со стороны ИИ из-за опоры на исторические данные. Такие предубеждения могут привести к неоправданному нацеливанию на определенные социальные группы, что приведет к непропорциональному полицейскому контролю.

Более того, предиктивные возможности ИИ могут ошибочно классифицировать людей на основе общих шаблонов данных. Такие обобщения способны нарушить фундаментальный принцип «невиновен, пока не доказана вина», вызвать обоснованные опасения относительно права на справедливый суд.

Чтобы способствовать сбалансированной интеграции ИИ в эту критическую парадигму, у правоохранительных органов есть ряд возможностей. Во-первых, это проведение комплексных аудитов, важность которых невозможно переоценить. Каждая система ИИ перед ее активным внедрением в правоохранительные органы должна пройти глубокую оценку. Хотя техническая надежность этих систем имеет важное значение, не менее важно обеспечить их соответствие нормативным актам, таким как этические принципы для надежного ИИ, введенные Группой экспертов высокого уровня по ИИ. Только выявляя и устраняя любые предубеждения на этом этапе, мы можем заложить основу для справедливого и беспристрастного внедрения ИИ.

Во-вторых, это содействие вовлечению сообщества. Некоторые сообщества часто оказываются исключенными из основного потока технологических достижений, сталкиваясь в результате с непреднамеренными негативными последствиями. Благодаря постоянному диалогу с этими сообществами правоохранительные органы могут собирать уникальные точки зрения, отличные от чисто технических оценок[1].

[1] Об этических проблемах применения ИИ и других технологий в борьбе с преступностью см.: *Демиденко А.* Киберэтика: Границы морали в цифровом мире. 2025. URL: https://mybook.ru/author/artem-demidenko/kiberetika-granicy-morali-v-cifrovom-mire/read.

Глава 7. Направления использования искусственного интеллекта в борьбе с преступностью

§ 1. Биометрия и распознавание лиц в правоохранительной деятельности

В эпоху, когда идентификация и проверка личности имеют первостепенное значение, биометрические технологии стали ключевыми инструментами в арсенале правоохранительных органов. Биометрические технологии позволяют идентифицировать людей, используя их уникальные физиологические (например, черты лица, отпечатки пальцев, рисунок радужной оболочки глаза) или поведенческие (например, походка, почерк) характеристики.

Распознавание лиц. До начала 1960-х гг. процедура была в основном ручной, полагались на индивидуальное восприятие и способность человека узнавать знакомые лица. Однако достижения в области технологий обработки изображений и компьютерной науки сделали возможным автоматическое распознавание лиц. Теперь компьютерные алгоритмы помогают полиции, а цифровые изображения, полученные различными способами, давно заменили печатные фотографии.

Эта технология использует алгоритмы извлечения и анализа определенных черт лица из изображений или видео для сопоставления и проверки идентичности. Она стала бесценным инструментом для правоохранительных органов.

Например, технология помогает быстро идентифицировать подозреваемых, сравнивая данные о лицах, собранные в ходе уголовного расследования, с историческими данными или базами данных преступников, доступными полиции. Кроме того, она играет важную роль в поиске пропавших людей, в том числе детей, сопоставляя изображения неопознанных лиц с базами данных пропавших без вести. Более того, вне контекста правоохранительных органов распознавание лиц обеспечивает повышенную безопасность в контролируемых средах, устраняя необходимость в традиционных методах аутентификации, таких как контроль физического доступа.

Однако рост распознавания лиц также сопровождался опасениями. В частности, предвзятость остается темой для дискуссий. Некоторые исследования выявили различия в эффективности системы, особенно при идентификации лиц из определенных этнических групп, полов или возрастных групп. Конфиденциальность и защита данных выделяются как еще одна значительная проблема. Поскольку системы распознавания лиц становятся повсеместными, особенно в общественных

местах, они вызывают дебаты об этических границах наблюдения и потенциальном неправомерном использовании. Более того, хранилища данных, которые питают системы распознавания лиц, могут быть привлекательными целями для кибератак, что подчеркивает важность надежных мер защиты данных.

В этом контексте крайне важно различать системы, используемые в режиме реального времени в общественных местах (распознавание лиц в реальном времени, англ. live facial recognition, LFR), и системы, используемые ретроспективно (распознавание лиц после события, англ. automated face recognition, AFR).

Вместо того чтобы фокусироваться на одном человеке, LFR выполняет считывание в реальном времени всех людей, проходящих мимо камеры, и сравнивает их с заранее определенным закрытым списком наблюдения лиц, представляющих интерес. В некоторых сценариях система будет немедленно отбрасывать изображения, которые не вызвали никаких результатов, чтобы избежать необоснованного нарушения применимых законов о защите данных. Приложения LFR создают значительные проблемы как с технической, так и с человеческой точки зрения (нагрузка на систему, человеческие возможности и предубеждения и т. д.). Полицейские силы в Великобритании и некоторых странах ЕС опробовали приложения LFR с разной степенью успеха.

При ретроспективном использовании AFR помогает следователям сравнивать изображения неизвестных лиц, например, кого-то, пойманного на видеозаписи системы видеонаблюдения, подозреваемого в совершении преступления, или фото арестованного, с базой данных. Эта база данных обычно контролируется и хранится законным образом, в нее могут входить изображения, полученные во время содержания под стражей или в ходе уголовного судопроизводства.

Направления распознавания лиц в полиции:

— *установление личности неизвестной персоны:* технологии биометрической идентификации, в частности распознавание лиц, играют решающую роль в работе правоохранительных органов по быстрой и эффективной идентификации неизвестных лиц. Два основных сценария в этом контексте:

1) расследование нераскрытых преступлений: при расследовании дела об убийстве кадры видеонаблюдения идентифицируют подозреваемого, что приводит к поиску изображения лица в базе данных известных и неизвестных лиц. Если первоначальные результаты отрицательные, то изображение все равно сохраняется. Два года спустя биометрический запрос вызывает совпадение во время другого расследования убийства, в итоге связывая подозреваемого с более ранним делом. Это демонстрирует силу биометрии в раскрытии дел с течением времени;

2) раскрытие сетей детской эксплуатации: в другом сценарии полиция конфискует компьютер сексуального преступника, инициируя биометрический анализ извлеченных изображений. Совпадения с жертвами из предыдущих расследований помогают раскрыть более широкую сеть преступников, вовлеченных в эксплуатацию детей;

— *целенаправленный поиск разыскиваемого человека:* правоохранительные органы в значительной степени полагаются на целенаправленный поиск известных лиц для проверки личности и оценки потенциальной причастности к преступлению;

— *раскрытие связей с террористами:* гражданин предоставляет анонимную информацию, связывающую определенного человека с серьезными преступлениями и терроризмом. Традиционный поиск по биографическим данным не дает результатов, что приводит к поиску по изображению лица. Это выявляет потенциальное совпадение с разыскиваемым террористом (иллюстрация того, как биометрия может усилить улики и помочь в борьбе с терроризмом);

— *раскрытие преступных сетей с помощью анализа мобильных данных:* эксперты-криминалисты анализируют смартфон подозреваемого, используя распознавание лиц для кластеризации медиа и сужения целей. Последующие поиски в биометрических базах данных известных или неизвестных лиц выявляют потенциальные контакты, что приводит к раскрытию более широкой преступной сети;

— *борьба с сетями финансового мошенничества:* в случаях мошенничества с банкоматами правоохранительные органы используют распознавание лиц, чтобы связать известного преступника с коллекцией изображений неизвестных мошенников. Этот целевой поиск помогает оценить участие известного преступника в дополнительных преступных действиях.

Биометрия в России. По данным ВЦИОМ (2025 г.), более 76% молодых людей поддерживают применение биометрии, в том числе для аренды самокатов, онлайн-кредитования и защиты покупателей на маркетплейсах. При этом 35% старшего поколения пока не готовы к сбору биометрических данных.

В России действует Единая биометрическая система (ЕБС) — государственная платформа, которая позволяет идентифицировать гражданина удаленно по его биометрическим данным. Основные задачи ЕБС: подтверждение личности без предъявления паспорта; удаленное

оформление услуг; усиление цифровой безопасности; экономия времени при получении государственных и коммерческих сервисов.

В августе 2025 г. были внесены изменения в ряд актов Правительства РФ по вопросам использования биометрических персональных данных, размещенных физическими лицами в единой биометрической системе с использованием мобильного приложения.

В частности, изменениями предусматривается механизм очного подтверждения в банке биометрических персональных данных, размещенных в ЕБС самостоятельно физическим лицом с использованием мобильного приложения. Установлено, что биометрические персональные данные иностранцев, размещенные в ЕБС, могут быть подтверждены оператором ЕБС посредством проверки их соответствия биометрическим персональным данным, которые были собраны и переданы в ЕБС при прохождении иностранцем пограничного контроля при въезде в Российскую Федерацию.

Также расширен перечень случаев использования биометрических персональных данных, размещенных физическими лицами в ЕБС с использованием мобильного приложения. Такие биометрические персональные данные могут использоваться: для заселения в гостиницу, санаторий, дом отдыха, пансионат, кемпинг, на туристскую базу или в иное подобное учреждение; осуществления аутентификации при проходе на объекты спорта и спортивные мероприятия; проведения идентификации заявителя — физического лица в целях создания удостоверяющим центром сертификатов ключей проверки электронных подписей и выдачи таких сертификатов и т. д.

Кроме того, биометрические персональные данные, размещенные в мобильном приложении и подтвержденные в установленном порядке в банке или оператором ЕБС, могут использоваться также: для предоставления государственных и муниципальных услуг при личном приеме в МФЦ (внесенными изменениями определен перечень услуг, при предоставлении которых допускается установление личности физического лица при личном приеме в МФЦ с использованием биометрических персональных данных, размещенных в ЕБС); осуществления безналичных расчетов в организациях торговли и сферы услуг, уплаты налогов, сборов, страховых взносов и иных платежей; проведения идентификации и (или) аутентификации физического лица в целях заключения или изменения договора об оказании услуг связи и проч.

Искусственный интеллект упростит регистрацию биометрии на портале «Госуслуги». Такую разработку внедрили в мобильное приложение «Госуслуги Биометрия». Она должна помочь быстро пройти процедуру регистрации даже тем гражданам, кто далек от новых технологий. Интеллектуальная система распознавания работает в режиме реального времени, отслеживая важные моменты записи видеосъемки. Она контролирует освещение, положение головы, угол съемки и наличие посторонних лиц в кадре, помогая человеку записать качественное видео, необходимое для успешной верификации.

Биометрические системы превосходят человеческие способности по точности распознавания лиц и голосов. Например, операционисты банков редко замечают различия между близнецами, тогда как специальные алгоритмы делают это почти наверняка. Современные решения используют комплексный подход: помимо анализа внешности учитываются индивидуальные особенности голоса. Дополнительно система сверяется с информацией, зафиксированной в профиле пользователя на портале «Госуслуги», где хранятся уникальные паспортные данные и СНИЛС. Благодаря этому вероятность ошибочной идентификации практически исключена.

Биометрия становится все более распространенной. Сейчас с ее помощью можно:

— открыть счет или оформить кредит в банке;

— получить электронную подпись;

— заселиться в гостиницу без паспорта;

— оплатить проезд в метро Москвы, Казани, Екатеринбурга, Самары, Нижнего Новгорода;

— зарегистрировать бизнес;

— получить сим-карту;

— подтвердить право на пенсию из любой точки мира;

— проходить в бизнес-залы аэропортов и т. д.

В ритейле первые автоматы по продаже энергетиков и табачной продукции уже используют технологию распознавания лиц для подтверждения возраста. С 1 сентября 2025 г. пассажирам предоставлена возможность применять биометрию для посадки на поезда дальнего следования. В 2025 г. появился и единый сервис оплаты по лицу. Его разработчики — Сбербанк и Национальная система платежных карт. Пользоваться им могут клиенты любых банков вне зависимости от того, какая организация обслуживает конкретную торговую точку. А в аэропорту Пулково запущен «зеленый коридор» для пассажиров с подтвержденной биометрией. Более того, с середины 2026 г. биометрия будет использоваться при совершении сделок с недвижимостью.

Виды биометрии:

— *упрощенная* — доступна через приложение «Госуслуги Биометрия». Подходит для базовых действий — вход в личный кабинет или оплата в метро;

— *стандартная* — требует загранпаспорта нового образца и телефона с NFC. Дает доступ к более широкому спектру услуг;

— *подтвержденная* — регистрируется в банке или МФЦ. Позволяет использовать биометрию для максимально защищенных операций, например сделок с недвижимостью.

Так, при совершении сделок с недвижимостью идентификация через биометрию будет проводиться в онлайн-режиме через портал «Госуслуги»:

— продавец и покупатель заходят на сайт Росреестра;

— загружают необходимые документы;

— подписывают их усиленной квалифицированной электронной подписью;

— проходят идентификацию через ЕБС (по лицу и голосу);

— если данные подтверждены — сделка проходит регистрацию.

Ни личное присутствие, ни бумажные заявления не нужны. Система сравнит лицо и голос пользователя с уже имеющимися данными в ЕБС. Это избавит участников сделок от необходимости подавать бумажные заявления в МФЦ. Раньше без них Росреестр просто не регистрировал электронные договоры.

По мнению разработчиков, новый подход не снижает, а усиливает защиту сделок. Ранее проверка ограничивалась электронной подписью. Теперь добавляется биометрия, причем в двойном формате: лицо + голос. Используются технологии liveness (в переводе с англ. — живость) — они позволяют отличить живого человека от фотографии, видео или дипфейка. А голос проверяется в реальном времени — пользователь должен произнести случайные цифры, так что записанный звук использовать не получится.

Доля электронных регистраций недвижимости в России уже приближается к 90%, отметили в Росреестре. Переход к биометрии — логичный шаг к более безопасным и удобным цифровым сервисам. При этом очные процедуры остаются доступными — тем, кто не готов к цифровому формату, можно по-прежнему обращаться в МФЦ и пользоваться услугами нотариуса.

Биометрическая идентификация против кибермошенничества. С 1 марта 2026 г. вступают в силу изменения о противодействии цифровому мошенничеству, где биометрия занимает центральное место.

Новый закон[1] вводит ряд цифровых ограничений и мер безопасности, направленных на защиту персональных данных граждан и предотвращение хищений через онлайн-сервисы.

Одна из ключевых новелл — возможность использовать биометрическую идентификацию при получении микрозаймов. Это означает, что гражданин сможет подтвердить свою личность с помощью лица и голоса, исключив возможность оформления займа посторонними лицами.

Также Закон закрепляет использование биометрии в системе госуслуг. При смене пароля на портале пользователь сначала получит уведомление о попытке изменения, а затем — код подтверждения. Такой подход добавляет еще один уровень защиты от неправомерного доступа к аккаунту.

Законодательство дополняется запретами на использование иностранных мессенджеров для коммуникации между банками, государственными органами и клиентами. В том числе усиливается контроль за идентификацией звонков — на экране будет отображаться реальное название организации. Это минимизирует случаи подмены номеров и телефонного мошенничества.

С 1 июля 2025 г. иностранным гражданам, не прошедшим регистрацию в ЕБС, стали постепенно ограничивать мобильные услуги. Срок действия старых контрактов истек, и теперь провайдеры начинают отключать сервисы нарушителям. Номера, которыми не пользовались более трех месяцев, блокируются. Остальные мобильные устройства ждет двухэтапное ограничение: сначала исчезает роуминг и уменьшается скорость Интернета, а спустя месяц прекращаются все услуги. Переоформить контракт пользователь может до момента полного отключения. Абоненты, находящиеся в стране, вправе обновить старые договоры, проверив количество активных номеров через портал «Госуслуги», закрыв ненужные и подтвердив личность в ближайшем салоне связи посредством биометрии из ЕБС.

С 30 июня 2025 г. граждане других стран, желающие приехать в Россию, обязаны пройти предварительную регистрацию через мобильное приложение ruID. На пограничном контроле им выдадут цифровые профили с присвоенным номером СНИЛС и подтвержденной учетной записью на портале «Госуслуги». Завершить регистрацию можно будет уже в Российской Федерации, посетив банк. Там же можно сразу

[1] Федеральный закон от 1 апреля 2025 г. № 41-ФЗ «О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации».

зарегистрироваться в ЕБС и получить остальные необходимые документы.

Регулирование и риски цифровой идентификации. Сбор биометрии возможен только с письменного согласия. Такое правило предусмотрено Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных». Исключения есть для отдельных случаев, прежде всего связанных с безопасностью или судебными решениями. Так, обработку биометрических персональных данных могут проводить без согласия субъекта персональных данных в следующих ситуациях:

— при реализации международных договоров Российской Федерации о реадмиссии;

— в связи с правосудием и исполнением судебных актов;

— при проведении обязательной государственной дактилоскопической регистрации;

— при обязательной государственной геномной регистрации;

— в случаях, предусмотренных законодательством об обороне, безопасности, противодействии терроризму и коррупции, оперативно-розыскной деятельности, нотариате, гражданстве, порядке въезда и выезда, государственной службе, уголовно-исполнительной системе (ч. 2 ст. 11 Федерального закона «О персональных данных»).

За нарушение порядка сбора биометрических данных предусмотрены штрафы: от 100 тыс. до 300 тыс. руб. — для должностных лиц; от 500 тыс. до 1 млн руб. — для юрических лиц (ст. 13.11[3] КоАП РФ). Вся биометрия хранится в Единой биометрической системе, которая работает как защищенное хранилище. Но ни одна система не застрахована от взлома. Утечка таких данных не просто неприятность, а реальная угроза: на их основе можно создавать дипфейки и проводить финансовые махинации.

Для противодействия этим угрозам разрабатываются специальные технологии:

— *технология liveness*. Биометрию невозможно «обмануть» снимком из соцсетей. Алгоритмы умеют отличать лицо живого человека от фотографии, видеозаписи или дипфейка. Проверяются: моргание; повороты головы; изменение мимики;

— *бимодальная биометрия*. Одновременно проверяются и лицо, и голос. Запись из соцсетей не поможет: система просит произносить случайные цифры, что невозможно подделать заранее;

— *сравнение с ЕБС*. Биометрические данные хранятся в государственной защищенной системе. Это делает невозможным участие подставных лиц или использование фальшивых данных.

§ 2. Новые технологии прогнозирования преступности и преступного поведения

Предиктивная полиция. Алгоритмическая полицейская деятельность — предиктивная полиция (англ. predictive policing) относится к системам и алгоритмам ИИ, которые предназначены для указания областей, мест и времени, в которых могут произойти определенные виды преступлений. Иногда их даже используют для прогнозирования того, кто может совершить преступное деяние.

Предиктивная полиция использует возможности больших данных для разработки прогнозных профилей людей на основе прошлой преступной деятельности, текущих ассоциаций и других факторов, которые коррелируют с криминальной склонностью. Алгоритмически сгенерированные «горячие точки преступности», как правило, являются местами, где живут и работают группы меньшинств.

Полицейские проверки и инциденты возвращаются в данные о преступности (поскольку они не основаны на разумных подозрениях) и могут влиять на дальнейший прогнозный анализ, что приводит к петле обратной связи, в которой одни и те же области и профили неоднократно подвергаются контролю.

Это явление известно в криминологии как синдром Люхова — Данненберга: увеличение присутствия полиции в определенном месте приводит к увеличению статистически зарегистрированных правонарушений и преступлений. Иначе говоря, большее присутствие полиции приводит к увеличению преступности. Предположительно, много преступлений в других сферах приходится оставлять «незамеченными», так как ресурсы полиции усилены в алгоритмически обозначенных областях.

Из-за отсутствия общедоступных оценок и подробностей о входных данных и функционировании этих алгоритмических и автоматизированных систем анализа данных существует множество примеров того, как такие системы прямо или косвенно приводят к расовому профилированию, расизму и другим формам дискриминации, особенно в отношении мусульман и людей, воспринимаемых как мигранты.

Действующие системы могут создать ложное подозрение и привести к наблюдению, посещениям полицией рабочих мест или дома, допросам, остановке текущих процедур предоставления убежища или даже к арестам, депортации и превентивному задержанию. Все это может произойти без каких-либо объективных доказательств уголовных правонарушений — только на основе данных, алгоритмически сгенерирован-

ных подозрений (характерный пример — война с незаконными мигрантами в США в период второго президентского срока Д. Трампа).

Алгоритмическая полицейская деятельность нацелена и на путешественников: информационная система Passenger Name Record (PNR) применяется к рейсам, прибывающим из третьих стран в страны ЕС. Директива ЕС PNR[1] позволяет хранить и обрабатывать все данные всех пассажиров рейса без доказательств какого-либо предыдущего преступного деяния или подозрений в течение шести месяцев. Такие данные о пассажирах включают всю информацию, которую необходимо предоставить при бронировании рейса, например продолжительность поездки и пункт назначения, номер кредитной карты, контактные данные, запросы на питание и замечания о конкретных потребностях, таких как помощь из-за инвалидности. Алгоритмы, основанные на предположениях полиции, ищут предположительно заметные закономерности в записях имен пассажиров. Какие закономерности полиция считает подозрительными, публично не известно. Люди, отмеченные как подозрительные, могут быть помещены под наблюдение или арестованы, их статус проживания может быть расследован или им может быть отказано во въезде в страну.

Распространение Palantir в правоохранительной деятельности и проблемы предвзятости. Программное обеспечение американской компании Palantir Technologies Inc. доступно во многих странах и помогает полицейским быстро искать и анализировать большие объемы данных. Система позволяет получать доступ и объединять сведения из нескольких полицейских баз данных, например, если человека останавливала, допрашивала или обыскивала полиция, или сведения из внешних источников, таких как социальные сети, мобильные устройства или сотовая связь. Система также позволяет профилировать и ориентироваться на людей, в отношении которых нет доказательств причастности к преступлениям, людей, не подозреваемых в совершении преступлений, и даже потерпевших и свидетелей.

Системы профилирования данных Palantir были протестированы или даже использовались не только без четкой, но и вообще без какой-либо правовой основы. Полицейские силы и структуры по защите данных часто расходятся во мнениях относительно объема и законности использования подобных систем. Программное обеспечение Palantir объединяет различные пулы данных, которые были собраны для совершенно разных целей, для создания сложных и подробных личных профилей, что может привести к иллюзорным корреляциям. Люди могут подвергаться произвольным преследованиям со стороны полиции, а поскольку они не знают об анализируемых данных, лишаются права защищать себя.

[1] Директива 2016/681/ЕС от 27 апреля 2016 г. об использовании данных системы бронирования (PNR) для предотвращения, выявления, расследования и уголовного преследования преступлений террористической направленности и тяжких преступлений.

Правительство Великобритании с 2025 г. разрабатывает программу «прогнозов убийств», которая, как оно надеется, сможет использовать персональные данные тех, кто известен властям, для выявления людей, которые с наибольшей вероятностью станут убийцами.

Утверждается, что исследователи используют алгоритмы для анализа информации тысяч людей, в том числе жертв преступлений, пытаясь выявить тех, кто подвергается наибольшему риску совершения серьезных насильственных преступлений.

Первоначально схема называлась «domicide project», но ее название было изменено на «sharing data» для улучшения оценки рисков. В рамках проекта будут использоваться данные людей, не осужденных за какие-либо уголовные преступления, включая личную информацию о членовредительстве и подробности, касающиеся домашнего насилия.

Схема будет проверять характеристики правонарушителей, которые повышают риск совершения убийства, и изучать альтернативные и инновационные методы обработки данных для оценки риска убийств.

Типы обрабатываемой информации включают имена, даты рождения, пол и этническую принадлежность, а также номер, идентифицирующий людей на национальном компьютере полиции. Раздел с пометкой «тип персональных данных, которыми будет делиться полиция с правительством», включает в себя различные виды уголовных судимостей, в нем также указан возраст, в котором человек впервые появился в качестве жертвы, в том числе домашнего насилия, и возраст, в котором человек впервые попал в поле зрения полиции.

Должны быть переданы — и перечислены в «специальных категориях персональных данных» — маркеры здоровья, которые, как ожидается, будут иметь значительную прогностическую силу (данные, касающиеся психического здоровья, зависимостей, склонности к самоубийству и членовредительству, инвалидности).

§ 3. Роботы и криминологические проблемы

Роботы — это порождение ИИ. Вряд ли чешский писатель К. Чапек, который в 1921 г. придумал слово «робот» (чешск. robot — выполняющий тяжелую работу, крепостной) для описания мыслящей машины,

мало отличимой от человека, мог предвидеть, что меньше чем через 100 лет тема робототехники станет одной из наиболее востребованных среди бизнес-сообщества, военных кругов, университетов и органов государственной власти, а теперь и криминологов.

В настоящее время в международном сообществе существует терминологический разнобой, связанный с применением таких категорий, как «автономные автоматизированные системы» и «роботы». Например, в документах ООН и Министерства обороны США используются в основном термины «автономные автоматизированные системы (ААС)» и «автономные смертоносные системы вооружений (АССВ)». В то же время бизнес, средства массовой информации в Соединенных Штатах и официальные документы НАТО и ЕС используют термины «роботы», «роботы-убийцы», «роботизированное оружие» и т. п.

При всей близости ААС и роботов они являются терминами, обозначающими различные технические и программные устройства. Большинство специалистов в области информационных технологий и робототехники придерживаются следующей точки зрения: «ААС» являются более широким термином, чем «роботы»; ААС включают в себя программно-технические комплексы с различной степенью автоматизации; в свою очередь, роботы представляют собой высокоавтоматизированные ААС.

Продемонстрируем это на понятном примере. Так называемые беспилотные летательные аппараты (БПЛА), или дроны, без сомнения, с первых своих образцов должны быть отнесены к ААС. Однако нельзя забывать, что до последнего времени подавляющая часть дронов предполагала наличие оператора, который не только принимает решения о применении вооружений, но и в отдельных случаях дистанционно пилотирует дрон. В этом случае, конечно же, ни о каком роботе речь идти не может. Такие дроны не являются роботами, хотя и представляют собой ААС.

Теория автоматического управления уже к 60-м гг. прошлого века выработала эффективный критерий, позволяющий надежно выделять роботов в структуре ААС. Данным критерием является способ принятия решения, требующегося в тех случаях, когда перед программно-аппаратным комплексом встает необходимость сделать выбор из нескольких альтернатив. Любой программно-аппаратный комплекс независимо от своего функционального предназначения должен быть способен выполнять как минимум две операции: перемещаться в пространстве и реализовывать свою функцию, например эвакуации раненых, разминирования, получения информации, огневого поражения и т. п.

Соответственно, принципиально возможны четыре комбинации в принятии решений: первая — все решения дистанционно принимает оператор ААС; вторая — все решения принимаются программным комплексом ААС без участия человека; третья — решения относительно всех операций ААС могут приниматься как человеком, так и программным комплексом; четвертая — на различных стадиях и человек, и программный комплекс могут принимать решения, но решение человека или программного комплекса на каждой из операций имеет окончательный приоритет.

Без сомнения, к роботам можно отнести второй тип ААС и с некоторой натяжкой третий. Далее в тексте в тех случаях, когда будет использоваться специально термин «роботы», он будет использоваться в отношении ААС второго и третьего типов. Во всех остальных случаях термин «ААС» будет подразумевать все типы роботов.

Можно выделить следующие основные направления использования ААС и робототехники деструктивными организациями.

Разведка. До последнего времени использование радиотехнической, электронной, воздушной, подводной и иной технологически сложной разведки было прерогативой исключительно государственных структур, включая разведывательные службы, правоохранительные органы и т. п. В настоящее время положение дел коренным образом изменилось. Впервые в истории деструктивные организованные структуры получили возможность ведения разведки по своей технической сложности, а соответственно и объему и качеству получаемой и обрабатываемой информации, не уступающей государственным структурам. В решающей степени это связано не только с распространением и развитием Интернета, но и с качественным скачком в развитии ААС и робототехники. Если еще несколько лет назад БПЛА, оснащенный универсальным разведывательным комплексом, включающим системы видеоразведки, наблюдения в инфракрасном диапазоне, средства перехвата телекоммуникационных сигналов, стоил 300—350 тыс. долл. США и изготавливался исключительно компаниями — подрядчиками Пентагона, то уже сегодня, а тем более завтра ситуация будет иная. В настоящее время такой комплекс может быть приобретен на легальном и нелегальном рынках любым платежеспособным клиентом, включая преступные и экстремистские структуры, менее чем за 50 тыс. долл. США. При этом изготовителями таких дронов-разведчиков-наблюдателей уже сегодня являются более 700 легальных компаний по всему миру, включая страны Азии, Африки, и неизвестное число нелегальных производителей.

Также сегодня доступны для деструктивных структур передвижные наземные разведывательные комплексы, монтируемые на автомобили и маскируемые под внедорожники, минивэны, фургоны и т. п. Данные комплексы, которые (без цены автомобиля) можно приобрести в различных странах мира легально и на «черном» глобальном рынке, стоят от 15 до 30 тыс. долл. США. Они позволяют не только прослушивать информацию из закрытых помещений, используя акустические эффекты, но и снимать информацию с расположенных в зоне действия комплекса компьютеров, планшетов и т. п. В Великобритании одной из преступных групп был заказан и использован разведывательный комплекс, который, будучи поставлен недалеко от банка-хранилища, позволял получать коды электронных банковских ячеек, снимая информацию при их открытии законопослушными клиентами.

Можно сделать прогноз, что в течение ближайших трех — пяти лет основная часть разведывательных комплексов, находящихся в руках деструктивных организаций, будет относиться к средствам воздушного и наземного базирования, соответственно, к дронам и разведывательным автомобилям. В более отдаленной перспективе следует ожидать освоение деструктивными структурами морских глубин и космического пространства.

Транспорт. Было бы удивительно, если бы преступные группы не воспользовались наиболее быстроразвивающимся сегментом военной и гражданской робототехники, а именно роботизированными транспортными средствами, не говоря уже о военном использовании автоматизированного транспорта для экспедиционных, эвакуационных и логистических нужд. Начиная с 2023 г. ежегодно увеличивается объем мирового рынка беспилотных автомобилей — роботов.

Известно, что любая высокая технология имеет тройное применение — военное, гражданское и криминальное, поэтому есть все основания полагать, что наиболее активно будут применять транспортных роботов террористы и преступные синдикаты.

Применительно к террористам данный тезис не нуждается в дополнительной аргументации. Террористические структуры, в том числе сетевого и роевого типа, уже сегодня имеют ресурсные технологические возможности, превосходящие потенциал многих государственных армий. В связи с этим террористы быстро и эффективно используют все виды вооружений и техники, которые применяются в современных армиях.

Что касается преступных транснациональных организаций, то использование транспортной робототехники позволяет им решить две

важные задачи. С одной стороны, оно дает возможность разнообразить каналы доставки тех или иных грузов и свести к минимуму человеческий фактор в этом процессе.

Самый страшный сценарий связан с размещением на беспилотниках биологического, химического или радиологического оружия. Появление и быстрый прогресс транспортных дронов резко расширит географию преступности, особенно в части наркотрафика, контрабанды и, возможно, рынка торговли человеческими органами.

Роботы-коммандос: они являются гибридом разведывательных и транспортных робототехнических систем, оснащенных средствами выполнения и других целевых функций. Например, такие роботы способны взбираться по вертикальным поверхностям, бесшумно проникать в закрытые помещения и т. п.

Основные факторы робототехники, значимые для криминологического анализа

Технологизация уличной и неорганизованной преступности. Традиционно использование сложных технических устройств и приспособлений являлось прерогативой организованной преступности. В последние годы ситуация коренным образом изменилась. С появлением Интернета вещей, по сути, весь окружающий мир превратился из мира вещей в мир ААС. Это в полной мере относится не только к сегодняшним сложным системам управления домом, но и к телевизорам, холодильникам, пылесосам, автомобилям и т. п. В ближайшие пять — семь лет ожидается появление массового рынка бытовой робототехники. Из дорогостоящих игрушек и статусных устройств для богатых бытовые роботы станут обязательной принадлежностью дома и квартиры средней семьи.

М. Гудман в книге «Будущее преступности» (Future Crimes, 2015) приводит пример, произошедший на Тайване в середине 2014 г. Полиция попыталась арестовать известного наркоторговца, который окружил свой дом сетью роботов-видеонаблюдателей, вооруженных поражающими электрошоковыми устройствами и слезоточивым газом. Обескураженная полиция столкнулась с необычным сопротивлением, а наркоторговец скрылся через заранее подготовленный подземный ход.

В последние годы по экспоненте растет число преступлений — от грабежей до убийств — с использованием ААС. Значительная часть подобных преступлений, зафиксированных в полицейских отчетах, остается нераскрытой. Это связано с тем, что подобные высокотехнологичные преступления, совершаемые отдельными лицами или не-

большими криминальными группами, в корне отличаются от традиционных правонарушений. Правонарушения, с которыми привыкла иметь дело полиция, полностью происходят в реальном мире. Соответственно, преступник оставляет улики, более того, он фиксируется в прошлом свидетелями, а в последние годы различного рода системами видеонаблюдения.

Преступность с использованием ААС и роботов предполагает, безусловно, физические действия. Но сигнал, который приводит в действие те или иные аппаратные средства, передается в электромагнитной среде и носит виртуальный характер. Сегодня для того, чтобы совершить преступление, не надо присутствовать на его месте. Можно находиться не за десятки, а даже за сотни и тысячи километров. Правоохранительные органы не привыкли работать в таких условиях, и, соответственно, их деятельность не слишком эффективна.

Не говоря уже о преступных синдикатах, даже отдельные уличные преступники отдают себе отчет в неспособности полиции противостоять высокотехнологичным преступлениям. Именно поэтому они берут на вооружение ААС и роботов как орудия преступлений.

Например, российские киберпреступники стали применять новый способ хищения данных банковских карт с помощью внешних интерактивных голосовых ответов (англ. interactive voice response, IVR). Мошенники используют специально запрограммированных роботов, звонящих клиентам финансовых организаций. Программа выдает себя за сотрудника банка и без труда выведывает всю необходимую информацию (учетные данные, PIN-коды, CVV-коды и т. д.).

Как правило, IVR используются для ответа на входящие звонки (приветствия клиентов, предложения перезвонить на внутренний номер сотрудника банка и проч.). Мошенники стали применять данную технологию для исходящих звонков. Представившись сотрудником финансовой организации, робот просит ничего не подозревающего абонента сообщить данные либо для уточнения некоторых моментов, либо из-за сбоя системы.

С целью скрыть свои следы злоумышленники запускают роботов в облачных дата-центрах (центрах хранения и обработки данных). Для того чтобы избежать подозрений со стороны жертв, время от времени программа перенаправляет их звонки на живых людей. Данная схема весьма эффективна, поскольку большинство клиентов банков не догадываются о способности роботов звонить.

Повышение вероятности крупномасштабных террористических актов. Длительное время крупномасштабные террористические акты

требовали долгой подготовки, вовлечения множества участников, затрат значительных и разнообразных ресурсов и, наконец, физического присутствия террористов в зоне актов устрашения и насилия.

Однако с повсеместным внедрением ААС, а в последующем робототехнических комплексов ситуация резко и неблагоприятно изменилась. В последние годы происходит активная автоматизация и роботизация производственной сферы и сферы обеспечения жизнедеятельности. Наряду с повышением технической надежности и экономией затрат этот процесс влечет и крайне негативные последствия. Сегодня в развитых странах мира жизнь миллионов людей, фактически всего населения страны, решающим образом зависит от объектов и сетей критической инфраструктуры. В их число входят не только федеральные объекты государственного управления и т. п., но и практически все системы жизнеобеспечения, включая энергетику, тепло- и водоснабжение, связь и т. д.

Энергетические сети, независимо от того, в чьей собственности и юрисдикции они находятся, управляются ААС, соединенными с Интернетом, как и системы городских водопроводов, канализации, теплоснабжения. Самое опасное состоит в том, что за последние пять — семь лет эффективными роботизированными системами оснащены все АЭС, крупнейшие плотины и т. п.

В связи с этим даже не тревогу, а ужас у специалистов в США вызвали известия о том, что за последние годы неопознанные хакеры неоднократно вторгались в систему энергоснабжения, комплексы автоматизированного управления и хранилища данных гидросооружений и даже атомных станций этой страны. В результате у неизвестных лиц или организаций имеется федеральная информация об уязвимостях и недостатках систем управления и обеспечения безопасности всех плотин и гидротехнических комплексов на территории США, систем водоснабжения многих крупных и крупнейших городов страны, региональных энергосистем.

В случае же если информация об уязвимостях в критических инфраструктурах и системах управления ими уже попала или попадет в распоряжение террористических организаций, экстремистских сообществ и с несколько меньшим риском — преступных синдикатов, могут произойти непредсказуемые по своим последствиям акты. Причем на сегодняшний день у структур национальной безопасности нет способов предотвратить их. Более того, затруднена будет идентификация нападающего.

Новые измерения финансового терроризма и преступности. Если на потребительском рынке продаются первые мелкосерийные полно-

ценные роботы, а в военной сфере на вооружение поступают первые единичные образцы, то в сфере финансов полностью роботизированные системы — торговые роботы — за последние годы стали обычными на большинстве финансовых рынков.

Торговые роботы представляют собой интеллектуальные программно-аппаратные комплексы, которые оснащены не только модулями сбора, обработки, анализа информации, но и самостоятельного, без человека, принятия решений сообразно алгоритмам. На последнее хотелось бы обратить особое внимание. Не только среди политиков, военных и бизнесменов, но даже среди части специалистов по информационным технологиям бытует заблуждение, что торговые роботы представляют собой предтечу ИИ и вплотную приблизились к нему. Внешне дело выглядит именно таким образом, поскольку все решения о купле-продаже акций, индексов, валют, деривативов и т. п. принимают непосредственно программно-аппаратные комплексы — торговые роботы. Но если обратиться к сути дела, то выяснится, что решения они принимают не по правилам, которые создали сами, а по алгоритмам, которые заложены в них людьми, — программистами, разработчиками, математиками, аналитиками и т. п. Поэтому об ИИ говорить пока преждевременно, хотя решения на финансовых рынках принимаются роботами без непосредственного участия человека.

Экспансия торговых роботов связана с двумя обстоятельствами. С одной стороны, торговля на финансовых рынках требует регулярной обработки огромных массивов информации. При краткосрочном трейдинге, а на него приходится основная часть операций, люди просто не успевают обработать и проанализировать разнородные и разноформатные массивы информации. Более эффективно это делают торговые роботы, которые принимают решения на основе некоторых правил. В этом смысле торговые роботы являются наследниками и более универсальными вариантами компьютеров, которые в прошлом обыгрывали чемпионов мира по шахматам. В обоих случаях в основе программ лежат определенные алгоритмические правила, построенные на основе иерархии принятия решений.

Автоматизированные системы способны быстрее людей реагировать на любую внешнюю информацию. Соответственно, с середины 2010-х гг. стали создаваться не только все более совершенные алгоритмически, но и все более быстродействующие торговые роботы.

Господство торговых роботов на финансовых рынках создало новые угрозы для финансовой системы и национальной безопасности. Исследования показывают, что колебания на финансовых рынках сейчас не обусловлены какими-либо событиями или новостными поводами, связанными с соответствующими компаниями. Эти колебания — результат действий торговых роботов, принимавших решения о купле-продаже в соответствии с некоторыми алгоритмами. В большинстве случаев торговые роботы принимали ошибочные решения в том смысле, что действовали не по алгоритмам, а в результате заражения специальными зловредными программами, срок существования которых измерялся секундами.

Во всех случаях имело место не просто хакерство, а тщательно спланированные и виртуозно осуществленные финансовые преступления с использованием программно-аппаратных комплексов. Доступные исследователям и общественности факты говорят о том, что с каждым годом количество и масштабы такого рода преступности, связанной с заражением, а в будущем, возможно, и перехватом управления торговыми роботами, будет только нарастать.

Применение роботов в борьбе с преступностью

В начале июля 2016 г. полицейского робота впервые использовали для убийства преступника: в Далласе был подорван подозреваемый в стрельбе по полицейским. Полиция решилась на использование робота для убийства преступника, так как тот отказался вести переговоры с правоохранительными органами. К гаражу, где скрывался стрелок, направили робота, обычно используемого для обезвреживания взрывных устройств. Робот не предназначен для убийства, но может переносить небольшое количество взрывчатки, потому что при необходимости подрывает большие подозрительные предметы. В этот раз к нему прикрепили примерно 450 г пластичного взрывчатого вещества военного назначения С-4. Этого хватило, чтобы при детонации на небольшом расстоянии от преступника нанести ему травмы, несовместимые с жизнью. Сам робот практически не пострадал: была повреждена только длинная «рука», переносящая дополнительный груз.

По словам эксперта в области военных технологий и автора книги «Изменяющийся характер войны» (Wired for War, 2009) П. Сингера, американцы впервые использовали такую тактику внутри страны, но за рубежом американские роботы уже убивали. В Ираке военные много раз использовали в качестве самостоятельного взрывного устройства недорогого робота MARCbot (он стоит около 15 тыс. долл. США). В Далласе взрыв устроил более мощный робот Remotec Androx Mark V A-1, который был приобретен полицией в 2008 г. за 151 тыс. долл. США. Помимо обезвреживания бомб он может разбивать окна, рас-

пылять слезоточивый газ, перерезать провода, пилить и проделывать отверстия. Робот не самостоятелен, каждое действие контролирует человек за пультом.

Помимо Remotec Androx Mark V A-1 в американской полиции «служит» и большое количество других роботов. Наиболее популярны роботы, подрывающие подозрительные предметы и деактивирующие взрывные устройства; их использование военными заметно увеличилось во время войн в Афганистане и Ираке.

Как правило, полиция выбирает компактные модели, чтобы они могли пролезать под машины и проникать в различные помещения. Часто роботы снабжены микрофонами и двумя-четырьмя камерами, передающими изображения в центр управления, а также мощными сенсорами, определяющими химический состав бомбы. Полиция активно использует модель PackBot 510 с детектором Fido, который «нюхает» бомбу и быстро определяет тип взрывчатки. От этого зависит выбор дальнейшей тактики — подрыв или обезвреживание на месте.

Иногда роботы помогают полиции не рисковать и действовать максимально аккуратно при захвате заложников. Простые модели, снабженные панорамными камерами и мощными микрофонами, позволяют оценить количество заложников и обстановку внутри здания, вести переговоры с захватчиками, а также доставлять еду и медикаменты по требованию.

Сложные роботы-разведчики, например BOZ1, могут вскрывать двери, проламывать стены и разбивать стекла, чтобы проникнуть в закрытые помещения. Еще более мощный робот Dragon Runner, разработанный компанией QinetiQ по заказу Пентагона, умеет подниматься по лестницам, двигать механической рукой, фиксировать движения людей и подслушивать их разговоры на довольно большом расстоянии. Однажды в штате Северная Каролина (США) этот робот пробрался к вооруженному мужчине, который заперся в своем доме и не сдался даже после пуска слезоточивого газа. Первый аппарат преступник разбил на мелкие кусочки, но когда приехал второй, между мужчиной и полицией начались переговоры (через камеру и микрофон у робота).

Другой робот в Альбукерке, штат Нью-Мексико (США), подобрался к мужчине, который забаррикадировался в своем доме и угрожал самоубийством. Аппарат при помощи манипулятора сбросил с него одеяло, чтобы убедиться, что тот не вооружен, и только после этого в дом вбежали полицейские.

В 2024 г. в г. Лаббок, штат Техас (США), произошел инцидент, который наглядно продемонстрировал, как роботы помогают стражам

порядка в борьбе с преступностью. 39-летний Ф. Делароза, подозреваемый в совершении преступления, забаррикадировался в номере мотеля Lubbock Days Inn и открыл огонь по прибывшим на место полицейским. Попытки переговорщиков SWAT убедить преступника сдаться окончились неудачей — в ответ Делароза вновь применил оружие. Тогда было принято решение задействовать робота-сапера, который используется полицией для обезвреживания взрывных устройств и опасных предметов. Робот, управляемый дистанционно, сумел проникнуть в номер через окно и распылить внутри слезоточивый газ. Преступник, пытаясь спастись от едкого дыма, выпрыгнул наружу прямо под колеса железного стража порядка. Многотонная машина придавила злоумышленника, пресекая возможную попытку бегства.

Отдельный тип роботов помогает полиции оценивать обстановку в условиях очень плохой видимости, например в абсолютной темноте, перед тем как направить наряд полиции в темную квартиру, где могут скрываться подозреваемые. Благодаря специальной оптической системе он позволяет оператору, сидящему за пультом управления, четко видеть то, что недоступно человеческому взгляду. Это существенно упрощает проведение рискованных полицейских операций.

Роботы сильно изменили проведение полицейских операций. Например, в Германии действуют роботы-саперы нового уровня. Сотрудникам правоохранительных органов даже не придется приближаться к подозрительным предметам, оставленным на улице: машина сама просканирует вещи и создаст 3D-модель закрытой сумки. Работа аварийно-спасательных служб сведется к просмотру готовых кадров на компьютере: инженеры должны будут проанализировать полученную картинку, сделать выводы о том, есть ли там бомба, и дать роботам следующие задания в зависимости от ситуации.

В Дубае самостоятельные роботы-полицейские следят за безопасностью на улицах, в парках и торговых центрах. Правда, все роботы безоружны, так что в экстренной ситуации не смогут вмешаться, а только передадут информацию полиции. Роботы, наделенные ИИ, предоставляют справочную информацию на шести языках, умеют шутить и заботиться о детях.

И совсем из области фантастики, которая фактически стала явью, — киборги. Исследователи из Университета Вашингтона в Сент-Луисе, штат Миссури (США) превращают насекомых в киборгов, которых можно отправить куда угодно для вынюхивания взрывчатки. Работы ведутся по заказу ВМС США. Исследователи изучают, как насекомые анализируют запахи. Установлено, что саранча может идентифицировать

конкретные запахи, которые ее научили обнаруживать даже при наличии посторонних запахов. Насекомые-киборги будут более эффективными, чем роботы, потому что они используют массу природных датчиков.

Даже самые передовые миниатюрные химические устройства используют всего несколько датчиков. Вместе с тем, если посмотреть на антенну насекомых, то там несколько сотен тысяч датчиков различных типов. Для того, чтобы превратить обычную саранчу в машину по поиску взрывчатки, инженеры планируют вживить в ее мозг электроды, чтобы подключиться к антеннам в виде усиков и расшифровать электрические сигналы. Так как операторы должны получать информацию, собранную насекомыми, исследователи также разрабатывают крошечный рюкзачок, который может передавать данные. На приемнике будет загораться красный светодиод при наличии взрывчатых веществ, в то время как зеленый свет будет сигнализировать об отсутствии угрозы.

И, наконец, инженеры планируют нанести татуировку на крылья насекомых с помощью биосовместимого шелка, способного преобразовывать свет в тепло. Лазер, который, вероятно, будет в рюкзаке, позволит оператору контролировать действия киборга. Фокусирование лазера на левом крыле обеспечит движение насекомого влево, и наоборот. Насекомое будет функционировать так же, как дистанционно управляемый дрон.

§ 4. Дроны, искусственный интеллект и борьба с преступностью

В книге «Будущее преступности» М. Гудман приводит такой пример: в 2013—2014 гг. на 80% сократился браконьерский отстрел слонов и носорогов в Африке. Секрет открывался просто. Американское правительство и корпорация Google в порядке гуманитарной помощи африканским странам, особо страдающим от браконьерства, предоставили подразделение патрульных и боевых дронов и обучили местный обслуживающий персонал обращению с этим грозным оружием. Единственной модификацией боевых дронов, используемых против браконьеров, было то, что с них были сняты огневые установки и установлены липучие сети и поражающие дротики со снотворным.

Полицейские США используют дроны и в более сложных операциях, например таких, как наблюдение за потенциально опасными преступниками.

Британские полицейские начали использовать практически бесшумные мультикоптеры Black Hawk, позволяющие вести видеозапись со звуком. Также британская полиция использует беспилотники в операциях по преследованию преступников. По различным оценкам, это обходится силовикам намного дешевле и безопаснее, чем применение мотоциклов, машин и вертолетов. Покупка дрона и его длительная эксплуатация обойдутся в сумму меньшую, чем одна погоня с использованием вертолета (что возможно далеко не всегда) и двух полицейских машин. Кроме того, применение беспилотников никак не угрожает жизни полицейских.

О первом успешном применении квадрокоптера британской полицией стало известно еще в феврале 2010 г., когда с помощью аппарата AirRobot AR100B, оснащенного системой видеонаблюдения и тепловизионной камерой, силовики графства Мерсисайд на западе Англии смогли разыскать в густом тумане автомобильного вора. Подобные дроны применяются в Великобритании до сих пор. Известно, что технология аппарата первоначально разрабатывалась для нужд военной разведки. Он практически бесшумный и может работать ночью, передавая изображение в режиме реального времени.

В настоящий момент беспилотники используются в правоохранительных органах целого ряда стран.

Во Франции и Японии беспилотники активно используются для дистанционного наблюдения за «скоплениями людей». Однако особый интерес вызывают отдельные подразделения, которые создаются в этих странах с целью борьбы со случаями несанкционированного использования дронов.

В России беспилотники различных типов стали использоваться полицейскими начиная с Олимпийских игр 2014 г. в Сочи. Дроны позволяют сотрудникам правопорядка эффективнее контролировать дорожную обстановку, проводить воздушную разведку, бороться с браконьерами и др.

Израильская компания Laser Detect Systems (LDS) представила первый в мире беспилотник SpectroDrone, оснащенный датчиками для определения взрывчатки и самодельных взрывных устройств с безопасного расстояния. Беспилотник использует разработанную компанией лазерную систему обнаружения взрывчатки и других опасных материалов в газах, жидкостях, порошках с расстояния в несколько километров. SpectroDrone способен выполнять эти задачи, имея оперативный радиус действия в три километра. Аппарат применяется для розыска баз и складов террористов, а также для обнаружения мин и

фугасов в зонах локальных конфликтов. В настоящее время для этих целей используют системы обнаружения взрывчатки, размещаемые на автомобильной технике, а также носимые комплекты и служебных собак.

В США к 2025 г. опыт работы с беспилотниками накоплен во всех 18 тыс. полицейских подразделениях.

Некоторые из сфер, где беспилотники особенно полезны:

— *наблюдение за подозреваемыми:* благодаря БПЛА можно выполнять съемку высокого разрешения и тепловизионную съемку. Это эффективно при слежке за потенциально опасными подозреваемыми. Собранные дроном данные могут быть проанализированы с помощью технологии распознавания лиц для быстрой идентификации подозреваемых.

Например, сотрудники полиции Брукхейвена, штат Нью-Йорк смогли задержать двух подозреваемых в ограблении с помощью беспилотника. Автомобиль нарушителей был идентифицирован считывателем номерных знаков возле местной аптеки на шоссе Буфорд.

Начальник полиции Брукхейвена дал комментарий об операции по поимке преступников и рассказал о шагах, которые привели к задержанию. Один из подозреваемых, обнаруженный возле аптеки, был арестован, в то время как другой бросился в бега. Воспользовавшись запасным выходом, он успел скрыться в лесу раньше, чем его настигли. Однако он не знал, что офицеры Брукхейвена уже отправили дрон для отслеживания его передвижений. Пилот полицейского дрона непрерывно передавал информацию своим коллегам во время операции по перехвату. В итоге офицерам удалось быстро задержать подозреваемого.

Дроны способны предоставлять полицейским ценную информацию в режиме реального времени для оперативного принятия аргументированных решений. Такой подход помогает обезопасить общественность и полицейских;

— *поисково-спасательные операции с дронами:* специальные дроны обладают тепловизором, лазерным дальномером, камерой с зумом и камерой с широкоугольным объективом. Также дрон может быть оснащен дополнительными аксессуарами. Например, динамиками и прожекторами, которые ускоряют спасательные операции. Динамики могут пригодиться, если пилот дрона обнаружит потерявшегося подростка, пожилого или любого другого человека (до его команды), обеспечивая уверенность в том, что помощь уже на подходе.

В России поисково-спасательный отряд «ЛизаАлерт» применяет для поиска пропавших людей беспилотники. Часто поисково-спасательные операции происходят в труднодоступной местности, в лесных массивах, иногда заболоченных участках. В таких случаях необходим тщательный обзор. Любая ошибка или промедление может стоить жизни. Для ускорения и повышения качества поиска специалисты отряда также включили в свою работу анализ с помощью нейросети. Иными словами, сначала беспилотник выполняет облет и съемку территории, где может находиться пострадавший. Затем все снимки с дрона передаются нейросети для оперативного анализа и определения любых следов, которые могут указывать на потерявшегося человека.

Беспилотные технологии и нейросети полностью трансформируют спасательные операции;

— *реконструкция места происшествия:* дроны оказываются полезными и для реконструкции дорожно-транспортных происшествий. Дроны обеспечивают сантиметровую точность, поскольку в них встроены специальные модули, точно учитывают следы заносов, поля обломков и другую ценную информацию, которая помогает в реконструкции аварии;

— *беспилотники для безопасности на массовых мероприятиях:* беспилотники обеспечивают дополнительные точки обзора во время проведения массовых мероприятий. Хотя традиционное патрулирование оправдано, дроны более эффективны и позволяют контролировать ситуацию в ситуациях с массовым скоплением людей, когда необходимо координировать их движение. Некоторые дроны оснащены динамиками в качестве дополнительных модулей, это может применяться для деэскалации насилия или идентификации, для предоставления помощи отдыхающим, которые могут потеряться, и т. д.;

— *дроны для мониторинга внутри помещений:* некоторые дроны специально разработаны для полетов внутри помещений или в небольших пространствах. Другие могут быть запущены с использованием специальной защиты лопастей. Например, в случае проведения операций в закрытых помещениях спецназу может пригодиться дополнительная пара глаз, чтобы убедиться, что локация чиста. Дроны направляют для разведки и оценки ситуации на место преступления. С помощью беспилотника можно определить количество нападающих и уровень вооружения, а также наличие заложников и оптимальный маршрут движения.

§ 5. Использование технологии блокчейн для предупреждения преступлений

В целях противодействия отмыванию денег и финансированию незаконной деятельности Росфинмониторинг совместно с Физическим институтом имени П. Н. Лебедева в 2020 г. разработал прототип системы для отслеживания криптовалютных транзакций в блокчейне биткоина. Проект получил название «Прозрачный блокчейн» и был внесен в федеральный проект «Искусственный интеллект».

В 2021 г. «Прозрачный блокчейн» начал работу. В том же году возбуждены первые уголовные дела благодаря системе отслеживания криптотранзакций. Росфинмониторинг начал сотрудничать в сфере отслеживания криптовалютных транзакций с Белоруссией, Мальтой, Лихтенштейном, Люксембургом и Финляндией.

В 2023 г. «Прозрачный блокчейн» был доработан совместно с Банком России и ВТБ. Помимо биткоина система получила поддержку более 30 цифровых активов. Систему активно используют правоохранительные органы.

«Прозрачный блокчейн» использован в закрытии даркнет-маркетплейса «Hydra» совместно с зарубежными коллегами. Система следит за «тысячами операций» с криптовалютой, проведено 120 расследований, возбуждено 60 уголовных дел. Несколько уголовных дел были доведены до судебных разбирательств при содействии «Прозрачного блокчейна». Наиболее резонансное — заказное убийство, оплаченное криптовалютой. Обнаружены факты оплаты цифровыми активами террористических актов. К системе начали подключаться центральноазиатские страны. Создана база серых адресов, их зафиксировано более 19 тыс.

В 2025 г. к «Прозрачному блокчейну» подключены российские банки, чтобы они имели возможность проводить комплаенс в реальном времени и связывать денежные переводы с криптовалютными транзакциями. К системе подключены более 12 тыс. пользователей (сотрудники правоохранительных органов и зарубежных подразделений антиотмывочной разведки). Начато создание реестра подозрительных криптовалютных адресов, принадлежащих россиянам.

Блокчейн действительно прозрачный. То есть вся информация о его работе публична и доступна всем без исключения.

Отслеживание транзакций в блокчейне осуществляется в несколько этапов.

Шаг 1 — сбор всех доступных данных. Создается обширная база данных, которая в реальном времени отслеживает несколько блокчейнов, выгружает из них все доступные данные. Особое внимание уделяется метаданным (временная метка, сумма перевода и т. д.).

Шаг 2 — составление графов и трассировка. На основе собранных данных составляются маршруты транзакций в виде графов (графических схем, демонстрирующих путь перемещения активов). Граф отображает связь адресов в блокчейне. Графическое представление связей упрощает процесс отслеживания перемещения криптовалюты.

Шаг 3 — кластеризация, выявление закономерностей и маркировка адресов. В первую очередь выявляются адреса, данные о которых можно получить публично: кошельки криптовалютных бирж (Binance, ByBit и др.), децентрализованных приложений (например, Uniswap), обменников, эмитентов активов (Tether, Circle, Paxos) и т. д. Этого уже хватает, чтобы охватить более 80% всех криптовалютных транзакций и частично их идентифицировать. Адреса обменников и бирж могут использоваться как точки входа/выхода (покупки или продажи криптовалют за фиат).

Стоит помнить, что крупные торговые платформы передают данные о своих клиентах правоохранительным органам, в том числе российским. Делается это по запросу с их стороны.

Шаг 4 — оценка рисков. На основе связей каждому адресу высчитывается уровень риска. Легальным криптовалютным сервисам присваивается низкий уровень риска (зеленый). Адресам неизвестного происхождения присваивается средний уровень риска (оранжевый). Высокий уровень риска (красный) присваивают адресам, которые использовались при взломах и похищениях криптовалюты, при мошенничестве и вымогательствах, в азартных играх, в даркнет-покупках, в смешивании криптовалюты при помощи специальных сервисов (миксеров), и адресам, включенным в санкционные списки.

Процесс идентификации личности. «Прозрачный блокчейн» может выявлять персональные данные жителей России и СНГ, которые покупают и продают криптовалюту. Это делается путем обнаружения связей между криптовалютными транзакциями и банковскими переводами. В этом процессе как раз и нужны собранные метаданные из блокчейна. Они сопоставляются с метаданными, полученными из банковских организаций.

Работает это примерно так:

— система обнаруживает транзакцию в блокчейне;

— фиксируется точное время транзакции, участники и сумма перевода;

— далее происходит поиск похожих банковских транзакций, за основу берется сумма перевода (для российских банков — конвертированная в рубли), время транзакции и другие метаданные;

— в случае обнаружения похожей банковской транзакции у системы появляются персональные данные сторон сделки, которые она в дальнейшем будет использовать для маркировки криптовалютных адресов.

С недавних пор криптовалютные обменники начали разбивать фиатные платежи на несколько транзакций в качестве одного из способов обойти систему отслеживания. Но такой метод неэффективен, так как «Прозрачный блокчейн» и подобные ему сервисы способны анализировать все точки входа/выхода, т. е. находить связь транзакции в блокчейне сразу с несколькими банковскими операциями.

Среди криптовалютных обменников распространена практика массового использования так называемых дропов — банковских счетов, открытых на третьих лиц. Таким образом администраторы обменников скрывают собственные персональные данные и обходят лимиты на объем банковских переводов.

Механизм «Прозрачного блокчейна» технически не уступает аналогичным аналитическим сервисам вроде Chainalysis, Elliptic, TRM Labs и др. Но есть нюансы, которые делают «Прозрачный блокчейн» уникальной системой. В отличие от иных аналитических сервисов российская разработка является государственной собственностью и имеет прямую связь с банковской инфраструктурой. Благодаря этому «Прозрачный блокчейн» способен в реальном времени идентифицировать россиян и жителей ближайших стран, которые используют безналичные деньги для покупки и продажи криптовалют.

В «Прозрачном блокчейне» использован мировой опыт. Еще в 2016 г. Интерпол, Европол и Базельский институт управления договорились о создании совместной рабочей группы, специализирующейся на цифровых валютах. В задачу группы входит сбор и анализ информации о преступном использовании цифровых валют, расследование вопроса о хранении доходов, полученных преступным путем, организация ежегодных семинаров и встреч представителей трех ведомств и других учреждений, а также создание сети специалистов по биткойн-преступности.

§ 6. Предотвращение террористических актов: технологии, позволяющие видеть сквозь стены

В борьбе с терроризмом используются различные технологии, помогающие видеть сквозь стены. К таким технологиям, системам, устройствам относятся следующие.

1. *Обратно-рассеянное рентгеновское излучение (ОРРИ).* Это технология, при которой рентгеновские лучи от источника не проходят сквозь объект, а отражаются. Так как объект не надо просвечивать насквозь, возможно использовать излучение с интенсивностью на несколько порядков ниже, чем при проникающем излучении.

К числу веществ с малой атомной массой относятся взрывчатые и наркотические вещества, алкогольсодержащие жидкости, ткани тела человека. Это позволяет легко идентифицировать скрытые органические материалы или людей, которые могут представлять угрозу безопасности.

Использование технологии ОРРИ позволяет:

— получать изображения органических предметов, плохо различаемых при обычно используемой технологии проникающего рентгеновского изучения;

— размещать источник и приемники излучения в устройствах досмотра, расположенных с одной стороны от досматриваемого объекта;

— создавать за счет малой мощности излучения устройств, использующих данную технологию, системы, безопасные для операторов и других людей.

2. *Переносной радар «Голограф».* Обнаруживает людей и животных через стены, уже поступил на испытания в спецподразделения Вооруженных Сил РФ. Разработка Центрального научно-исследовательского института химии и механики предназначается для использования в контртеррористических операциях и должна помочь быстро скоординировать действия отряда и обезопасить заложников. Доработка устройства возможна после испытаний радара военными.

Это устройство в первую очередь необходимо подразделениям антитеррора, которые работают с учетом необходимости сохранения жизни заложников. Когда при выполнении операций надо обеспечить сохранность окружающих объектов, «Голограф» также окажет помощь бойцам спецназа.

Радар может спасти много жизней в ситуациях, когда есть какие-то материалы или объекты, которые нельзя повредить, например борт самолета, где приходится работать врукопашную. Благодаря радару

можно разобрать цели, посмотрев, кто где находится и где есть шанс неожиданно обрушиться на врага, — это 50% успеха.

Радар «Голограф» работает при помощи сверхкоротких радиоимпульсов на частоте от 1 до 4 ГГц, пропуская их через любые материалы и принимая отраженный сигнал, обнаруживает движение на расстоянии до 6,5 м. Устройство обладает небольшими габаритами и весом 4,5 кг, выдерживает падение на бетон с высоты 1 м и может использоваться при температурах от –20 °С до +50 °С.

«Голограф» способен распознавать движения сквозь кирпич, бетон, дерево, гипс, глину, сухой грунт и штукатурку. Главное, чтобы материал не содержал воды. Все зависит от материала стены — сквозь дерево он «видит» на метр, если это кирпич — на полметра, а бетон уже должен быть тоньше, потому что содержит железо. Кроме того, очень важно, насколько материал стены влажен: если это свежепостроенное здание и кирпич или пеноблоки не высохли, то видно хуже — волны гасятся, мешает вода.

Помимо сырого кирпича проблемой может стать совместное использование «Голографа» с устройствами, заглушающими сигналы сотовой связи. Данная возможность ограниченно испытана, при низкой мощности излучателей радар не реагирует на мобильные телефоны, Wi-Fi-роутеры.

Радар прост в использовании, предусмотрена возможность работы с помощью одной руки. Любой человек, даже новобранец, сможет пользоваться устройством через 15 минут после того, как ему объяснят принцип работы. В нем очень мало (практически нет) настроек — есть кнопка включения и очень доступная индикация.

3. *Технология визуализации с помощью Wi-Fi.* Компания Technische Universität Ilmenau (ФРГ) создала в 2017 г. уникальный высокочувствительный компактный прибор, который позволяет с высокой степенью детализации смотреть сквозь препятствия. Разработчики устройства утверждают, что оно дает возможность заглянуть за бетонные и кирпичные стены даже многометровой толщины.

Физики из Массачусетского технологического института (МТИ) придумали в 2016 г., как с помощью обычного Wi-Fi-передатчика видеть людей сквозь стены, причем не просто видеть, но даже определять вес и рост человека. Ученые из МТИ несколько преобразовали работу обычного Wi-Fi-маршрутизатора и «научили» его в буквальном смысле видеть объекты, находящиеся в соседней комнате. Технология работает довольно просто: маршрутизатор передает Wi-Fi-сигналы через стену, которые отражаются от предметов и возвращаются назад, отображая картинку на экране компьютера. Затем ученые «натаскали» модифицированные передатчики на распознавание человеческих силуэтов, а дальнейшее улучшение алгоритма привело к тому, что маршрутизаторы «научились» определять точный рост и вес человека.

Такая технология, по большому счету, уже достаточно давно известна, но, как признали ученые из Массачусетса, она была рудиментарной. Вопреки этому мнению, 23-летний студент из Мюнхенского технического университета Ф. Холл в 2017 г. доказал, что Wi-Fi уже достиг возможностей, позволяющих получать качественные голограммы или трехмерные фотографии объектов в другой комнате, используя лишь два небольших устройства. Ему потребовалось всего 20 секунд, чтобы сканировать в достаточно качественную объемную картинку все, что было у него за стеной. «Можно различить фигуру человека или собаку на кушетке, — пояснил разработчик, — любой предмет размером более четырех сантиметров». Чтобы «смотреть сквозь стену», Холл использовал лишь две крохотные антенны вроде тех, которыми оснащены обычные смартфоны. Полученная антеннами информация обрабатывалась специальной программой, которая выдавала ее в виде качественной 3D-голограммы.

4. *Прибор ночного видения, действующий на основе приема и распознания инфракрасного излучения*. Известны и «просвечивающие» сканеры, которые используют в аэропортах для поиска спрятанных под одеждой предметов. Но, скажем, для условий боевых действий нужно что-нибудь более «зрячее», способное на большом расстоянии распознавать противника, спрятавшегося не за фанерной ширмой или тканевым пологом, а за кирпичными стенами, панельными плитами и т. п.

5. *Сканирование при помощи радиоволн в терагерцевом диапазоне — Т-лучей*. Это разработка ученых Мэрилендского университета (США).

Приборы, использующие излучение такой частоты, уже применяются в медицине. В отличие от рентгеновских Т-лучи совершенно безвредны для биологических объектов. Сложность их использования заключается в том, что их применение до сих пор было возможно только при температурах, близких к абсолютному нулю. Есть проблема визуализации изображения, полученного отраженным от объекта Т-лучом. В медицине эта задача решалась при помощи пластин из графена — модификации углерода с повышенной подвижностью электронов в кристаллической решетке. Благодаря этому свойству Т-луч

получает возможность «нагреть» и «выбить» эти электроны из графеновой пластины, вследствие чего на пластине возникает положительный потенциал, который и помогает зарегистрировать и визуализировать исследуемый объект.

6. *Технология, основанная на эффекте Доплера*. Технологическая компания «ЭМИИА» (г. Симферополь) разработала прибор, использующий изменение частоты и длины волн, регистрируемых приемником, вызванное движением их источника и (или) движением приемника. В текущем виде система объединяет два компьютера и специальные сканирующие устройства.

В зависимости от типа и материала преграды система позволяет «смотреть» сквозь стены и другие оптически непрозрачные препятствия в радиусе до 50 м. В настоящее время изобретатели переносят свое детище на мобильную платформу и разрабатывают микрочип, который можно будет внедрять в различные аппараты и носимые гаджеты. В перспективе устройство может выглядеть как планшетный компьютер или шлем для бойца. Оно может устанавливаться на беспилотные летательные аппараты и передавать информацию на землю. Эта технология сможет заменить аварийные датчики и охранные устройства.

7. *Портативный радар — стеновизор*. Способен видеть людей даже через толстые стены. Изделие позволит спецназовцам вычислять террористов не только в зданиях, но и в замаскированных блиндажах и подземных тоннелях.

Новейший радар-стеновизор РО-900, разработанный группой компаний «Логис-Геотех», способен определять местонахождение движущегося человека на расстоянии до 21 м, при этом он видит сквозь несколько кирпичных или бетонных стен общей толщиной до 60 см. Это позволит бойцам Росгвардии на безопасном расстоянии обнаружить террористов не только внутри зданий, но и на их противоположной стороне, определить траекторию перемещения, а боевиков, стоящих неподвижно, радар обнаружит по дыханию.

Стеновизор РО-900 работает по принципу георадара-локатора, который способен проводить радиоволны не только по воздуху, но и через грунт и стены зданий и регистрировать все отражения от препятствий. Прибор похож на обыкновенную рацию без антенны. Он оснащен 3,5-дюймовым цветным дисплеем, который в реальном времени отображает результаты радиолокационной разведки. Полученные данные выводятся на экран в виде движущихся по диагонали красных полос — вертикальное направление экрана отображает информацию о расстоянии, на которое переместился человек, а горизонталь позволяет определить время, за которое он совершил маневр. При этом сам стеновизор очень компактен, его вес не превышает 1 кг.

Радар также регистрирует повторяющиеся движения с небольшой амплитудой, засекая таким образом расширение грудной клетки во время вдоха или биение сердца. Уже после 20 секунд анализа полученных данных радар выводит информацию об обнаружении затаившегося человека на дисплей в виде горизонтальной синей черты.

Эксперты считают, что стеновизор станет огромным подспорьем при боях или контртеррористических операциях в городах.

Группа исследователей из Массачусетского технологического института к 2025 г. создала инновационную систему визуализации под названием *mmNorm*, которая позволяет воссоздавать трехмерные модели объектов, скрытых за непрозрачными материалами. Технология использует сигналы миллиметрового диапазона, аналогичные применяемым в сетях Wi-Fi и 5G, для получения детальной информации о предметах, находящихся за препятствиями.

В отличие от традиционных радарных систем, которые могут определить лишь местоположение скрытого объекта и дать приблизительное представление о его форме, mmNorm обеспечивает значительно более высокую точность реконструкции. Основной принцип работы технологии заключается в анализе отражений беспроводных сигналов от поверхностей объектов под различными углами, что позволяет определять ориентацию и кривизну поверхности в каждой точке.

Во время тестирования система продемонстрировала точность реконструкции на уровне 96% для различных сложных предметов, включая столовые приборы и электроинструменты. Разработанная технология представляет собой принципиально новый подход к трехмерной реконструкции объектов и может иметь широкое практическое применение.

Роботы, оснащенные подобной системой, смогут не только обнаруживать предметы внутри закрытых контейнеров, но и определять их тип, ориентацию и состояние без необходимости открывать упаковку.

Потенциальные сферы применения технологии включают также системы безопасности в аэропортах, где mmNorm может повысить качество сканирования багажа и выявления запрещенных предметов.

§ 7. Глобальная навигационная система, электронное и спутниковое наблюдение в целях предотвращения преступности и терроризма

Глобальная навигационная система — это совокупность методов, программных и технических средств, позволяющих организовать фиксацию пространственно-временной информации и получение ее правоохранительными органами. Целью создания данной системы является повышение уровня информационно-аналитического обеспечения деятельности правоохранительных органов при осуществлении расследования и предупреждение преступлений[1].

Глобальная навигационная система представляет собой совокупность средств получения, а также программно-аппаратных комплексов обработки и передачи пространственно-временной информации. Комплекс средств получения пространственно-временной информации включает в себя следующие подсистемы: ГЛОНАСС, подсистему стационарной связи, подсистему мобильной связи, подсистему радиочастотной идентификации, подсистему видеофиксации, подсистемы фиксации фактов обращения и персонализации.

Подсистемы, входящие в состав глобальной навигационной системы, отличаются набором фиксируемых данных, принципами работы, а также формой представления полученной информации. Для оптимизации комплексного использования составных частей глобальной навигационной системы необходима интеграция всех массивов пространственно-временной информации, зафиксированной их средствами, в единый информационный комплекс. Однако различия в принципах фиксации пространственно-временной информации в системах с автоматической фиксацией данных (ГЛОНАСС, стационарные системы связи, системы мобильной связи, системы радиочастотной идентификации, системы видеофиксации) и системах фиксации фактов обращения и персонализации диктуют необходимость разделения алгоритмов их использования в интересах правоохранительной деятельности.

Для обеспечения оперативности получения пространственно-временной информации о контролируемых объектах, а также представления данной информации в удобном для визуального восприятия виде необходима интеграция систем с автоматической фиксацией данных

[1] См.: *Дусева Н. Ю.* Технико-криминалистические основы использования глобальной навигационной системы в расследовании и предупреждении преступлений: дис. ... канд. юрид. наук. Волгоград, 2015.

в единую структуру. Основой для данной интеграции могут служить существующие программно-технические комплексы систем мониторинга транспортных средств, функционирующие на основе спутниковой навигации, которая позволяет получать информацию о контролируемых объектах в виде карты с указанием их местонахождения в определенный момент времени. Одновременное отображение на карте местности пространственно-временной информации из всех систем с автоматической фиксацией данных позволяет провести упреждающие меры по пресечению преступлений.

С учетом назначения формируемой глобальной навигационной системы к перечню ее основных функциональных возможностей необходимо отнести: мониторинг контролируемых объектов, отображение местоположения контролируемых объектов на электронной карте местности, аналитическую обработку полученных данных.

Системы с автоматической регистрацией данных, входящие в состав глобальной навигационной системы, предполагают минимальное участие человека в процессе фиксации и хранения в них пространственно-временной и иной информации, что обеспечивает отсутствие «человеческого фактора» при ее обработке и сводит к минимуму ее возможные искажения.

В едином комплексе с глобальной навигационной системой следует рассматривать и новые *технологии электронного контроля*.

После событий 11 сентября 2001 г. создан ряд интересных *технологий дистанционной слежки*, которые могут найти повсеместное применение.

После ликвидации У. бен Ладена командой американского спецназа SEAL Team 6 в поле зрения журналистов попала секретная программа Пентагона под названием «Метки, отслеживание и поиск», или TTL. Целью этого проекта является создание средств, которые позволяют выследить особо важных лиц, скрывающихся в районе боевых действий или даже среди населения другой страны.

В настоящее время арсенал средств слежки охватывает практически все возможные способы идентификации и сопровождения человека: от классических сканеров отпечатков пальцев и радужки глаза до тепловой сигнатуры конкретного человека и микроскопической пыли, распыляемой с беспилотных самолетов и светящейся в лучах радаров.

Антитеррористическая батарейка. Первой и достаточно простой была технология инфракрасных маяков, которую используют как солдаты, так и секретные агенты. Маяк представляет собой программи-

руемую ИК-лампу, работающую в импульсном или непрерывном режиме, и источник питания. Свет, излучаемый таким маяком, не виден невооруженным глазом, но хорошо заметен в прибор ночного видения (ПНВ) или тепловизор. В июне 2009 г. «Аль-Каида»[1] выпустила электронную книгу, посвященную тактике шпионов из числа местного населения, которые работают на США. Среди описания действий вражеских агентов авторы публикуют фотографии инфракрасного маяка, приспособленного для работы от обычной девятивольтовой батарейки типа «Крона», которую несложно купить в Пакистане. В книге утверждается, что эти устройства пакистанские шпионы, нанятые американцами, используют для наведения беспилотных самолетов. Возможно, имеется в виду, что агенты таким образом, практически ничем не рискуя и не связываясь со своими «работодателями», помечают маяками автомобили и здания, где скрываются террористы.

Надо отметить, что похожие инфракрасные маяки используют и американские солдаты для того, чтобы пилоты вертолетов и операторы БПЛА могли отличить их от бойцов противника. Сегодня инфракрасные маяки уже морально устарели. Есть сообщения, что полевые агенты получили в распоряжение специальные мобильные телефоны, оснащенные встроенным инфракрасным лазером. В пыльном воздухе лазерный луч с большого расстояния виден в ПНВ или тепловизор, что позволяет агенту указывать на цель, не приближаясь к ней. Кроме того, такой «лазерный телефон» может в режиме реального времени давать целеуказание ракетам Hellfire, что потенциально снижает вероятность побочного ущерба.

Квантовая точка на карте. Чтобы отслеживать передвижение определенного человека и выделять его из толпы, американские военные разрабатывают специальную жидкость, которая позволяет обнаружить объект с большого расстояния.

Компания Voxtel разрабатывает продукт под названием NightMarks. Он представляет собой прозрачную жидкость, состоящую из крошечных нанокристаллических квантовых точек на основе селенида кадмия. Этот материал способен поглощать ультрафиолетовое (200—400 нм) или инфракрасное (700—1600 нм) излучение, а затем эффективно передавать энергию на специальные нанокристаллические люминофоры, которые светятся как в видимой (400—700 нм), так и в ближней инфракрасной области спектра.

[1] Террористическая организация, запрещенная в Российской Федерации.

Достаточно нанести такую жидкость на одежду или кожу человека (простым рукопожатием, с помощью БПЛА или другим способом), и беспилотный разведчик сможет надежно отслеживать яркую метку с большого расстояния. Эффектами поглощения и испускания света можно управлять, что позволяет изменить оптические свойства квантовых точек и создать множество своеобразных спектральных штрихкодов. Таким образом, появляется возможность отслеживать и надежно идентифицировать множество объектов.

Компания Tiax работает над аналогичными метками, которые могут со временем разлагаться. Это позволит избежать путаницы в большом количестве объектов наблюдения, а также снизить вероятность обнаружения факта слежки.

Использование RFID-чипов. Они похожи на те, что применяются в качестве метки для товаров в магазинах. В настоящее время армия США уже широко использует эту технологию идентификации своих сил на поле боя и логистики.

Специалисты Sandia National Laboratories разработали RFID-метки (англ. radio frequency identification, RFID), которые способны реагировать на радиолокационный импульс и с высокой точностью определять местоположение объекта слежки. Например, обычные чипы, используемые в магазинах, имеют дальность действия в несколько метров, в то время как RFID-метки от Sandia имеют радиус до 20 км. Особенностью технологии является высокая скрытность — метки «отзываются» только после облучения специальным радиолокационным импульсом.

Подобные RFID-чипы можно использовать не только для оперативной слежки за людьми и автотранспортом, но и в качестве превентивной меры по контролю за оружием, например встраивать их в переносные зенитные ракетные комплексы или противотанковые ракеты. В случае попадания этого оружия в руки террористов его будет достаточно легко обнаружить и быстро уничтожить ракетным ударом.

Миниатюрные RFID-метки могут работать с компактными радарами вроде M600 SpotterRF. Прибор размером с ноутбук разработан прежде всего для охраны периметра военных баз, но имеет большой потенциал для скрытой слежки; использует радиоволны X-диапазона и может обнаружить пешеходов на расстоянии до 1 км, а автотранспорт — до 1,5 км. Радар оснащен датчиком GPS и интегрирован с сервисом Google Earth, что позволяет отслеживать местоположение объекта на интерактивной карте.

Технологии уникальных запахов. Технологии оптического и радиолокационного слежения совершенны, но потенциально обнаружимы и поддаются обратному инжинирингу, т. е. враг может разобрать найденный маяк и придумать контрмеры. По этой причине военные ищут дополнительные способы тайной слежки. Технология компании Tracer Detection Technology предполагает использование уникальных запахов, позволяющих безошибочно выделить искомый объект из толпы. Специалисты компании изобрели специальный парафиновый карандаш, наполненный перфторуглеродами, термически стабильными соединениями, которые используются повсеместно — от производства холодильников до парфюмерии. Пары перфторуглеродов могут отслеживаться с помощью различных датчиков, например газового хроматографа. Достаточно провести карандашом по объекту слежки, и он в течение нескольких часов будет источать специфичный, незаметный для человеческого носа аромат. При этом изоляция в наглухо запертой комнате или под несколькими слоями одежды не поможет — по данным исследования, представленного в Министерство юстиции США, перфторуглеродные маркеры проникают сквозь закрытые окна, контейнеры и запертые чемоданы. Остаточные следы маркера сохраняются даже после тщательного смывания.

Технологии биомаркеров. В 2007 г. на одном из брифингов сил специальных операций США кратко упомянули об использовании в качестве технологии слежки биомаркеров — биологических веществ, которые позволяют надежно идентифицировать человека. Подробностей об этой технологии нет, судя по всему, она представляет собой протеин, в котором зашифрован определенный код-идентификатор.

На руке человека такая метка выглядит как обычный синяк, можно снять с себя всю одежду, тщательно вымыть тело и сбрить все волосы, но маленькая незаметная биометка позволит идентифицировать человека в любом случае. Тактика использования биомаркеров остается загадкой, особенно это касается считывания информации и внедрения биометки. Теоретически биомаркер может оставаться в человеке на всю жизнь, что позволяет быстро выявить террориста, который выдает себя за другого человека.

Технология трехмерного моделирования лица человека. Все описанные выше технологии имеют один существенный недостаток: нужно подобраться к преследуемому поближе. Однако это не всегда возможно.

Чтобы от подобного «невидимого ока» скрыться было совершенно невозможно, компания Photon-X разрабатывает технологию трехмерного моделирования лица человека по нескольким снимкам с оптических и инфракрасных камер беспилотников. Специальное программное обеспечение позволяет создать детальный профиль головы человека с помощью мультиспектральных датчиков и анализа движения лицевых мышц. Новая система позволит идентифицировать человека в толпе и сопровождать его без необходимости установки каких-либо маяков. Разумеется, оптические сенсоры не могут следить за человеком внутри здания, но зато они могут легко найти его даже на многолюдной улице большого города. Далее при необходимости врага можно уничтожить ракетой или привлечь агентов, которые установят маяк. Система Photon-X решает главную задачу — слежение за большим количеством людей на обширных пространствах.

Спутниковый мониторинг в борьбе с преступностью. Спутниковый мониторинг представляет собой процесс наблюдения за Землей с использованием искусственных спутников. Эти спутники оборудованы различными сенсорами и камерами, способными собирать данные в режиме реального времени. Сбор информации происходит в различных спектрах, включая видимый, инфракрасный и радиолокационный.

Направления использования спутникового мониторинга:

— *помощь в поисково-спасательных операциях.* Спутники могут быстро определить местоположение пропавших или потерпевших бедствие людей;

— *обнаружение нелегальных действий.* Спутниковый мониторинг позволяет эффективно выявлять незаконные действия, такие как нелегальная вырубка лесов, незаконная добыча полезных ископаемых и браконьерство. Высокое разрешение спутниковых снимков позволяет фиксировать изменения на поверхности Земли и анализировать их причины;

— *борьба с наркотрафиком.* Спутники могут обнаруживать плантации наркотических растений, а также отслеживать маршруты перевозки наркотиков. Благодаря этому правоохранительные органы получают возможность пресекать деятельность наркокартелей и изымать крупные партии запрещенных веществ;

— *контроль границ.* Охрана государственных границ — еще одна важная область применения спутникового мониторинга. Спутники могут отслеживать передвижения на пограничных территориях, выявлять нелегальных мигрантов и предотвращать контрабанду. Это осо-

бенно актуально для стран с протяженными границами, где наземное патрулирование затруднено.

Преимущества спутникового мониторинга:

— *высокая оперативность:* одним из ключевых преимуществ спутникового мониторинга является возможность получения данных в режиме реального времени. Это позволяет правоохранительным органам оперативно реагировать на возникающие угрозы и предотвращать преступления;

— *широкий охват территории:* спутники способны охватывать большие территории, что делает их незаменимыми в ситуациях, когда наземное патрулирование невозможно или затруднено. Это особенно важно в условиях сложного рельефа или труднодоступных районов;

— *точность и детальность данных:* современные спутники обеспечивают высокое разрешение снимков, а значит — возможность детально анализировать обстановку на земле. Это позволяет правоохранительным органам более эффективно планировать свои действия и принимать обоснованные решения.

Вызовы и ограничения спутникового мониторинга:

— *проблемы с разрешением:* несмотря на значительные достижения, разрешение спутниковых снимков все еще ограничено. В некоторых случаях детали могут быть недостаточно четкими для точной идентификации объектов, что затрудняет работу правоохранительных органов;

— *стоимость технологий:* запуск и обслуживание спутников — это дорогостоящий процесс. Кроме того, для эффективного использования спутниковых данных требуются специализированные программы и оборудование, что увеличивает затраты;

— *вопросы конфиденциальности:* использование спутникового мониторинга поднимает вопросы конфиденциальности и защиты персональных данных. Важно обеспечить, чтобы сбор информации не нарушал права граждан и соответствовал законодательству.

Перспективы развития спутникового мониторинга:

— *развитие технологий:* с развитием технологий спутниковый мониторинг станет еще более эффективным. Улучшение разрешения снимков, повышение скорости передачи данных для анализа информации откроют новые возможности для борьбы с преступностью;

— *международное сотрудничество:* для более эффективного использования спутниковых технологий необходимо развитие международного сотрудничества. Совместные усилия государств и обмен информацией помогут более эффективно противостоять глобальным угрозам;

— *этические и правовые аспекты:* важно также учитывать этические и правовые аспекты использования спутникового мониторинга. Необходимо разработать международные нормы и стандарты, которые обеспечат защиту прав граждан и предотвращение злоупотреблений.

Возможности программы спутникового слежения за мобильными телефонами. Современные GPS-технологии могут помочь выполнить поиск телефона, а также многих других объектов через спутник. Осуществляет все это спутниковая система, работающая через специальную программу слежения.

Если система слежения используется для наблюдения за людьми, то у наблюдаемого человека с собой всегда должно быть специальное устройство — персональный GPS-трекер или сотовый телефон фирм Nokia, iPhone, HTC с поддержкой функции GPS и операционной системой, например Android. Таким образом, этот мобильный телефон превратится в своеобразный «маячок» с установленной на нем специальной программой слежения. Если использовать программу слежения для наблюдения за людьми, то мобильный телефон легко можно положить в портфель или карман объекта, который нуждается в вашем контроле, или, если необходимо GPS-слежение за автомобилем, мобильный телефон можно положить и в «бардачок». После определения программой слежения точных координат, местонахождения и скорости данные отправляются на сервер системы. Все эти данные программа слежения получает с заранее заданной периодичностью.

Проследить за тем, как проводится GPS-слежение, можно в режиме онлайн: с компьютера или мобильного телефона. Помимо местонахождения наблюдаемого объекта в конкретный момент времени GPS-программа слежения позволяет на электронной карте проследить направление движения и его скорость. GPS-система слежения сохраняет всю историю передвижений отслеживаемых объектов.

Сегодня каждый желающий, вооружившись специальным программным обеспечением, имеет возможность проследить за действиями любого абонента сотовой связи, т. е. при помощи специальных программ, таких как ShadowGuard, например, можно прослушать переговоры по чужому телефону или же прочитать переписку по СМС. Еще несколько лет назад это было похоже на шпионскую фантастику, но сегодня это реальность, и огромное количество людей воспользовалось такой возможностью. А там, где имеется спрос, как известно из законов рынка, рождается и предложение. И на сегодняшний день появилось множество сервисов, которые предлагают воспользоваться такой невероятной возможностью.

Электронное антитеррористическое наблюдение. Серьезный шаг сделали и разведывательные технологии после событий 11 сентября 2001 г., когда были приняты беспрецедентные меры, даже охарактеризованные в СМИ как конец существования конфиденциальной информации в США. Особого внимания заслуживает крупномасштабный проект Министерства обороны США «Тотальная информационная осведомленность» (ТИО). Он предполагает разработку и эксплуатацию новейших ИКТ, с помощью которых можно осуществлять тотальное наблюдение за счет массированного увеличения источников информации, перехвата сообщений любого характера, оперативного анализа в режиме реального времени, т. е. сбора колоссального количества данных, а главное — молниеносную реакцию спецслужб. Эти меры должны противодействовать террористическим угрозам за счет мониторинга местонахождения, передвижений и деловой активности населения, т. е. сбора максимально широкой информации обо всех подозрительных явлениях, указывающих на планы террористов.

Система ТИО интегрирует всеобъемлющие цифровые данные об американских гражданах, а также об иностранцах, имеющих контакты с населением США, которые следует подразделить на два типа: личностные (деловые, функциональные) и биометрические. Первые предполагается черпать из всех существующих баз данных как государственного, так и отраслевого назначения: медицинских, образовательных, торговых, туристических, телефонных, корпоративных, ветеринарных и т. д., а также из источников, куда проникли все отслеживающие электронные устройства: банковские счета, кредитные карточки, аренда машин, транспортные агентства, медицинские и ветеринарные записи, телефонные и иные коммуникативные сообщения, письменные, электронные, телефонные заявления граждан в государственные органы и т. д. Биометрические данные — это изображение радужной оболочки и сетчатки глаз, отпечатки пальцев, ДНК, графические снимки лица и т. д.

Если учесть, что при этом используется хорошо зарекомендовавшая себя традиционная техника сбора данных, например просеивание телефонных счетов, магазинных дисконтных карточек и т. д., но уже через виртуальное сито, то сбор информации по линии ТИО достигнет беспрецедентных масштабов. Возникает уникальная централизованная система, которая содержит точные данные о том, где находился и что делал конкретный человек в заданное время.

Новый этап в эпоху слежения за объектами связан с космическими летательными аппаратами, в частности спутниками, возможности которых с учетом постоянно совершенствующейся фотовидеоаппаратуры безграничны. Причем передающие спутники могут двигаться по определенной траектории, фиксируя все на своем пути, а стационарные — предметы и их передвижение в одной географической точке. Спутники, оснащенные специальными приборами, не только видят, но и слышат, отслеживая разнообразные коммуникативные процессы. Это своеобразные динамические базы данных, они не только собирают и хранят информацию, но и могут отправлять ее на Землю в заданном режиме. Наличие кода предохраняет ее от расшифровки. Спутникам мирного назначения проложили дорогу спутники-шпионы, существующие уже более 40 лет, оснащенные обычными или инфракрасными фотокинотелекамерами, электрооптическими сканерами и иной аппаратурой, несущие свою службу и сейчас.

Вся Земля находится в зоне видимости космических аппаратов. Маршруты спутников ничем не ограничены, поэтому с их помощью любое государство способно заглядывать в «огород соседа», причем не одномоментно, а неограниченное время. Вероятно, с точки зрения военных и политических целей (например, для мониторинга того, как выполняются двусторонние или многосторонние государственные обязательства) они вряд ли заменимы.

В ряде стран, в первую очередь в США, созданы системы геопространственной разведки — прежде всего в целях национальной безопасности, а также использования в гражданских целях. Спутниковая геопространственная информация находит применение и в борьбе с терроризмом.

В Германии введена единая компьютерная антитеррористическая база данных. Этот информационный банк состоит из двух частей: основной и расширенной. В основную включен набор данных, необходимых для идентификации личности (имя, пол, дата рождения, адрес, гражданство, владение языками, цветная фотография и приметы подозреваемых в террористической деятельности). Доступ к этой информации получат все разведывательные органы и службы по борьбе с преступностью.

В расширенную базу введена информация о семейном положении подозреваемого, его профессии, образовании, конфессиональной принадлежности, номерах автомобилей, банковских счетов и телефонов; данные о передвижении по миру, принадлежности к террористическим ячейкам, навыках владения оружием и обращения со взрывчатыми веществами, круге общения, связях с террористическими ячейками. Эту информацию заинтересованные ведомства могут получать

по спецзапросу. Однако субъекты спецзапросов строго не оговорены. Тогда этот запрос могут организовать и сами террористы, выявив тем самым круг потенциальных сторонников и недоброжелателей. Кроме того, возможны «утечка» информации изнутри и взлом извне или то и другое вместе. Тогда тщательно собранная, всеобъемлющая информация может оказаться во власти посторонних людей, а главное — криминальных структур. Нетрудно представить удовлетворенность последних, когда нужная информация будет подана буквально «на блюдечке».

Разведывательные системы становятся все более универсальными: в автоматическом режиме они не только собирают информацию, но и осуществляют ее анализ, делают выводы. Именно так работают системы глобальной слежки: в ряде англоязычных стран — ECHELO, в Европе — ENFOPOL, у нас — СОРМ-2.

Революционным событием является возможность с помощью современных ИКТ обозревать не отдельные участки, регионы, а целиком планету. Совсем недавно произошел беспрецедентный в мировой истории случай, когда известная компания Google Earth выставила на сетевое обозрение все без исключения уголки планеты. Появилось множество информации об объектах, о которых никто не ведал, и даже о тех, которые скрывались, например о секретных базах, аэродромах, кораблях, подлодках и т. д. Посредством новейших просматривающих устройств современное человечество в конце концов сумело рассмотреть свою колыбель и место обитания — Землю — в зеркале, называемом электронной информацией.

Минцифры России в 2025 г. запустило сервис обработки с помощью ИИ видео с камер наблюдения из российских регионов. Сервис обеспечивает интеллектуальную обработку видеопотоков, позволяет получать, хранить и обрабатывать с применением ИИ (включая компьютерное зрение) видеоданные с камер наблюдения, поступающие из регионов.

Единая платформа видеонаблюдения позволит собрать видеопотоки с региональных платформ безопасных городов и регионов по всем субъектам страны, создать единый гибкий контакт-центр, который в случае возникновения чрезвычайных ситуаций позволит перекидывать голосовую нагрузку с одного субъекта на другой для того, чтобы люди могли дозвониться и получить необходимые консультации и необходимую поддержку.

В российских городах работает 1,2 млн камер видеонаблюдения, но лишь половина камер из тех, что установлены за счет государства, подключены к централизованным системам.

С технической точки зрения «умной» может быть абсолютно любая камера, только видео с нее надо отправить на сервер для обработки либо обработать на месте с помощью алгоритмов машинного зрения для поиска нужного объекта или действия.

Глава 8. Искусственный интеллект и борьба с коррупцией

§ 1. Российский и международный опыт использования искусственного интеллекта в борьбе с коррупцией

Президент России В. В. Путин заявил на международной конференции AIJourney (декабрь 2024 г.), что использование ИИ делает решения чиновников прозрачными.

В России ИИ использует государственная информационная система (ГИС) в области противодействия коррупции *«Посейдон».* Система была создана по Указу Президента России В. В. Путина в 2022 г.[1] С ее помощью можно собирать и анализировать сведения о доходах и имуществе чиновников.

Система «Посейдон» ориентирована на профилактику коррупционных правонарушений и использует данные Федеральной налоговой службы, Росимущества и Росфинмониторинга, а также информацию из социальных сетей. Ее применение позволяет сформировать своего рода цифровой профиль проверяемого лица и получить информацию о возможных конфликтах интересов: неформальном общении с представителями подконтрольных граждан, организаций и т. д.

Однако сам по себе факт обнаружения «Посейдоном» возможных коррупционных корреляций не является основанием для привлечения проверяемого лица к ответственности — только «сигналом» для возможной, но не обязательной проверки.

Разработки, связанные с применением ИИ, внедрены *в работу полиграфа и контрольно-надзорную деятельность.*

В лаборатории интеллектуальной аналитики Центра цифровых решений и ИИ РАНХиГС разработана *система анализа проектов нормативно-правовых актов на коррупциогенные факторы* — выборочн-

[1] Указ Президента РФ от 25 апреля 2022 г. № 232 «О государственной информационной системе в области противодействия коррупции «Посейдон» и о внесении изменений в некоторые акты Президента Российской Федерациии».

ное изменение объема права, чрезмерную свободу подзаконного нормотворчества, выход документа за пределы компетенции, неполноту административных процедур, отказ от конкурсных процедур и даже юридико-лингвистическую неопределенность. Оценка достоверности экспертизы, которую осуществляет эта система, уже достигает 75%.

Счетная палата РФ применяет ИИ для *анализа планов федеральных органов исполнительной власти по противодействию коррупции.* Исследование 2023 г. в отношении более 100 документов показало, что часть из них не соответствует общенациональным планам в данной области, причем трудозатраты на эту работу удалось сократить в 15—20 раз. Если на анализ документов «вручную» инспекторы затратили бы 300—400 человеко-дней, то с помощью ИИ вся работа была бы завершена за 20.

Лидеры стран — участниц Шанхайской организации сотрудничества (ШОС) выразили готовность работать над дальнейшим углублением взаимодействия в правовой и судебной областях, в том числе в рамках борьбы с коррупцией и реализации антимонопольного регулирования. Об этом говорится в тексте итоговой декларации саммита ШОС в Тяньцзине (1 сентября 2025 г.).

Участники саммита «продолжат координацию усилий в области борьбы с коррупцией и призывают международное сообщество отказаться от предоставления убежища лицам, совершившим коррупционные преступления». Согласно тексту декларации, государства — члены ШОС также признают важность взаимодействия в области антимонопольной политики и «намерены наращивать практическое сотрудничество по линии профильных ведомств».

Широкие возможности борьбы с коррупцией раскрывает использование искусственного интеллекта.

На саммите ШОС в Китае проблемам развития этой главной технологии новой промышленной революции было посвящено несколько принятых документов.

В связи с этим интерес представляет международный анализ этих процессов.

Самой большой международной новостью на этом направлении стало назначение в сентябре 2025 г. премьер-министром Албании *бота на основе искусственного интеллекта в качестве нового министра государственных закупок*. Бот «Диелла» будет контролировать и распределять все государственные тендеры, которые правительство назначает частным фирмам. Это первый член правительства, который физически не присутствует, а виртуально создан ИИ. Он, по замыслу, поможет сделать Албанию «страной, где государственные закупки на 100% свободны от коррупции».

В Глобальном антикоррупционном блоге (9 января 2025 г.) отмечается: «Инструменты искусственного интеллекта (ИИ), способные эффективно обрабатывать и анализировать огромные объемы данных, обладают огромным потенциалом для усиления мер по борьбе с коррупцией. Традиционные методы расследования, часто требующие обширного ручного анализа финансовых документов, контрактов и переписки, могут быть трудоемкими и подвержены человеческим ошибкам».

Системы на базе ИИ, особенно основанные на машинном обучении, способны анализировать большие наборы данных для выявления закономерностей и отклонений, выявляя потенциально коррупционные действия быстрее и точнее, чем следователи-люди. Некоторые из наиболее перспективных применений технологий ИИ в борьбе с коррупцией включают:

— *обнаружение аномалий в финансовых транзакциях:* используя сложные алгоритмы, системы ИИ могут распознавать закономерности подозрительных расходов, обнаруживать внезапные изменения в финансовом поведении и отмечать несоответствия, которые могут указывать на взяточничество, мошенничество или отмывание денег, а также значительно сокращать количество ложных срабатываний.

Например, после скандала с Global Laundromat банк HSBC внедрил системы ИИ, которые выявляли сложные схемы коррупции и мошенничества, анализируя огромные объемы данных, включая геолокацию, IP-адреса и шаблоны использования. Инструменты ИИ также могут оценивать взаимосвязи между счетами, клиентами и предприятиями, раскрывая скрытые связи, которые могут указывать на коррупционную деятельность. В банковском деле и финансах это помогает учреждениям выявлять риски, связанные с ведением бизнеса с определенными сторонами. Кроме того, ИИ может анализировать неструктурированные данные, такие как новостные статьи или сообщения в социальных сетях, чтобы помочь финансовым учреждениям и регулирующим органам раскрыть негативную информацию, которая может остаться незамеченной при использовании традиционных методов мониторинга;

— *мониторинг государственного сектора:* инструменты ИИ могут преобразовать методы контроля со стороны правительств по контрактам, процессам закупок и государственным расходам. Автоматизируя надзор, ИИ помогает выявлять конфликты интересов, фаворитизм и завышенные цены в государственных контрактах.

Например, в Бразилии была внедрена Система оценки рисков в сфере управления (англ. global risk assessment service, GRAS) Всемирного банка для выявления потенциальных коррупционных рисков в государственных закупках. GRAS анализирует обширные общедоступные наборы данных из списков избирателей, социальных программ, платежных ведомостей и компаний, занесенных в черные списки, для выявления доказательств сговора, неправомерного политического влияния и других тревожных сигналов. Подход GRAS, основанный на данных, позволил бразильским властям обнаружить коррупцию на миллионы долларов как на уровне штатов, так и на муниципальном уровне. Его прогностические возможности выходят за рамки государственных контрактов, помогая властям выявлять сети сговора и нетипичные схемы расходования средств в секторах с высоким уровнем риска;

— *предиктивная аналитика в правоохранительной деятельности:* ИИ также играет важную роль в предиктивной аналитике, помогая правоохранительным органам прогнозировать области, наиболее подверженные коррупции. Анализируя исторические данные о коррупционных делах, модели ИИ могут выявлять факторы риска, которые аналитики-люди могут упустить. Это позволяет правоохранительным органам сосредоточить ресурсы там, где вероятность коррупции наиболее высока. Например, инициатива Комиссии по ценным бумагам и биржам США «Прибыль на акцию» (EPS) использует ИИ для выявления нарушений в бухгалтерском учете и раскрытии информации, которые могут указывать на манипулирование доходами. Эта инициатива привела к многочисленным мерам принудительного характера.

Аналогичным образом, Министерство юстиции США успешно использовало аналитику ИИ в громких делах о коррупции за рубежом, таких как осуждение А. Мурильо, бывшего министра правительства Боливии, замешанного в многомиллионной схеме взяточничества. Анализ финансовых отчетов с помощью ИИ помог обнаружить финансовые аномалии и связи, которые в противном случае могли бы остаться незамеченными, что в итоге позволило Министерству юстиции найти доказательства того, что Мурильо получил более 500 тыс. долл. США в виде взяток, чтобы помочь флоридской компании заключить контракт на сумму 5,6 млн долл. США с Министерством обороны Боливии.

Необходимо быть бдительными и учитывать возможность того, что *сами коррупционеры будут использовать системы ИИ для достижения своих незаконных целей и подрывать усилия по борьбе с коррупцией.* Особенно серьезную угрозу может представлять способность систем ИИ создавать и усиливать дезинформацию. В Бангладеш фейковое видео, изображающее политика в сложной ситуации, стало вирусным, нанеся ущерб его репутации и подорвав доверие к демократическим процессам. Подобные инциденты подчеркивают масштаб угроз дезинформации, где ИИ используется для создания ложного, но убедительного контента с целью манипулирования общественным мнением, создания негативной репутации или отвлечения внимания от кампаний по борьбе с коррупцией.

Международный антикоррупционный исследовательский центр U4 в феврале 2025 г. выпустил аналитический доклад «Искусственный интеллект в борьбе с коррупцией — актуальные новости о технологиях ИИ», в котором эксперты U4 сосредоточили внимание на трех ключевых темах: 1) применение ИИ для борьбы с коррупцией в «классических» областях, где технология уже показала определенные достижения; 2) области, где ИИ был внедрен, но не дал положительных результатов; 3) некоторые перспективные области применения ИИ.

1. К «классическим» областям, где ИИ помогает эффективнее противодействовать коррупции, относятся мониторинг государственных закупок, борьба с мошенничеством и отмыванием денег, а также анализ больших данных. Успешное применение ИИ в этих областях обусловлено прежде всего его способностью масштабно обрабатывать и связывать неструктурированную информацию, а также гибким подходом к неконтролируемому обучению.

Например, *в сфере государственных закупок* ИИ позволяет:

— выявить новые (хотя бы теоретически) и скорректировать существующие индикаторы коррупции («красные флажки»);

— рассмотреть возможность использования гораздо более широкого набора входных данных при анализе и мониторинге закупок для выявления более сложных схем сговора и конфликтов интересов.

Что касается *выявления мошенничества и борьбы с отмыванием денег,* ИИ помогает превратить эпизодические выборочные проверки в более эффективные, комплексные и оперативные инструменты мониторинга. В отчете приведен пример глобального конгломерата по производству напитков, который консолидировал более десятка внутренних систем управления ресурсами предприятия с несколькими внешними потоками данных. Результатом стала консолидированная функция проверки поставщиков, поддерживаемая ИИ, которая позволила сократить расходы более чем на 90%.

С точки зрения обработки больших данных, ИИ позволяет *более эффективно выявлять и анализировать релевантную информацию.* Например, в Перу следователи используют ИИ для проверки растущего объема зарегистрированных подозрительных финансовых транзакций. Финансовый конгломерат HSBC удвоил показатель обнаружения подтвержденных незаконных транзакций и сократил время обработки транзакций с более чем месяца до нескольких дней.

2. Попытки использовать ИИ для принятия государственных решений с целью ограничения их дискреционных полномочий, порождающих коррупцию, не увенчались успехом. Было установлено, что системы ИИ выдают множество неверных или спорных решений: например, необоснованный отказ в выплате пособий по безработице тысячам законных претендентов в Мичигане, неправомерное лишение социальных пособий в Сербии и детских пособий голландским родителям. Этот недостаток связан со спецификой функционирования ИИ (непрозрачность принятия решений моделями машинного обучения, особенно сложными) и правом собственности на модели и данные ИИ. Невозможность полного объяснения решений ИИ нарушает один из основных принципов административной юстиции (принцип гласности и открытости).

Другая проблема заключается *в предвзятости обучающих данных и значительной склонности ИИ к «галлюцинациям» (выдумке и выдаче ложной информации за факт).* Даже системы ИИ, специализирующиеся на юридических вопросах, «галлюцинируют» в 30% случаев, например, ссылаясь на несуществующие правовые положения.

Все эти проблемы говорят о том, что ИИ может оказывать поддержку в принятии решений, но при этом человек как лицо, принимающее окончательное решение, является необходимым условием для достижения справедливых и точных результатов, а также для установления четких рамок ответственности в случае возникновения проблем.

3. *Новыми антикоррупционными возможностями для ИИ* авторы доклада называют *дистанционное зондирование и инклюзивное участие.*

За последние 10 лет *системы ИИ развили способность извлекать информацию из изображений и распознавать сложные закономерности.* Это открывает новые возможности использования ИИ для борьбы с рядом незаконных видов деятельности, тесно связанных с коррупцией, например с незаконной вырубкой леса. Так, компания Forest Foresight разработала технологию на основе ИИ, способную предсказывать незаконную вырубку лесов за несколько месяцев до ее начала.

В ходе экспериментального внедрения в Габоне она помогла инспекторам парка провести 34 мероприятия по обеспечению соблюдения правил и остановить незаконную добычу золота.

Кроме того, дистанционное зондирование с применением ИИ использовалось при:

— повышении производительности труда рейнджеров по обнаружению ловушек в Камбодже (в три раза);

— распределении ответственности за удаленные разливы нефти в Средиземном море;

— выявлении недобросовестных поставщиков при закупках в Бразилии;

— выявлении нелегальных майнеров биткоинов в Иране;

— пресечении незаконной рыболовной деятельности по всему миру;

— предотвращении выбросов метана в США и т. д.

Эксперты U4 считают столь же перспективным использование ИИ для защиты от «захвата политики» и содействия инклюзивному участию граждан в принятии государственных решений.

Помимо анализа сфер применения ИИ в целях противодействия коррупции, авторы публикации предлагают лицам, ответственным за разработку и реализацию соответствующих решений, учитывать *ряд сопутствующих особенностей и проблем.*

Необходимость решения проблем цифрового неравенства. Доступ к ИИ и исходные данные, используемые ИИ, неравномерно распределены по странам, гендерному, этническому и социально-экономическому признакам, например:

— только 22% специалистов в области ИИ — женщины;

— страны с высокой долей маргинализированных сообществ могут иметь низкую представленность в цифровой сфере;

— определенные группы лиц могут иметь непропорционально высокую заметность в отношении определенных неблагоприятных событий (например, более высокая распространенность в статистике преступлений из-за большего внимания полиции).

Это может привести к тому, что системы ИИ, вероятно, будут выдавать больше ошибочных и (или) предвзятых результатов: например, системы поддержки принятия решений на основе ИИ при найме персонала могут воспроизводить гендерное неравенство, полагаясь на устаревшие данные, которые смещены в сторону найма и продвижения кандидатов-мужчин. Важно учитывать эти особенности использования ИИ для анализа и принятия решений.

Возможность объединения разрозненных инициатив в области раскрытия информации, прозрачности и открытых данных с использованием ИИ. В Чехии, например, ИИ помогает выявлять длинные цепочки политических связей с данными о финансах и открытых правах собственности. Отдельные наборы данных ценны сами по себе, но в совокупности они позволяют выйти на новый уровень антикоррупционного анализа и мониторинга.

Важность инвестиций в целевые обучающие данные и модели открытого владения. Ограниченная доступность объективных данных является одним из основных препятствий для полного раскрытия потенциала ИИ, включая его применение в борьбе с коррупцией. Целенаправленная поддержка создания специальных общедоступных обучающих наборов данных в тесном сотрудничестве с профессиональным антикоррупционным сообществом может помочь раскрыть этот потенциал.

Необходимость разработки ресурсов и инфраструктуры для оспаривания несправедливых решений ИИ. Учитывая масштабы работы систем ИИ, даже в оптимальных условиях ИИ неизбежно будет выдавать большое количество ложноотрицательных результатов, т. е. ошибочно обвинять людей в мошенничестве, лишать их социальных льгот и т. д. Поэтому необходима поддержка пострадавших лиц, особенно из социально незащищенных групп — путем создания практических возможностей для пересмотра решений, подачи эффективных жалоб и, при необходимости, возбуждения судебных дел. Кроме того, может быть полезным инвестирование в аналитические инструменты и системы оценки, которые помогут определить, когда и как ИИ не справляется со своими задачами, выдавая предвзятые и ошибочные результаты.

Важность наращивания потенциала в области ИИ в более широком антикоррупционном сообществе, включая понимание его ограничений (предвзятости и «галлюцинации») и развитие навыков формулирования запросов к системам ИИ. Для создания целевых антикоррупционных продуктов необходимы эксперты, способные адаптировать существующие системы ИИ и обучить их работе с использованием соответствующих открытых данных. Поддержка со стороны государственных органов, гражданского общества и доноров также важна в этом смысле для консолидации ресурсов, поддержки технического потенциала и сохранения прагматичного подхода к оценке эффективности ИИ, а также выявления областей, где необходимы передовые технологии, и областей, где достаточно простых решений.

А. Лопес Асера, руководитель отдела агентства Валенсии по борьбе с мошенничеством, AVAF, в статье на сайте агентства (21 ноября 2023 г.) указывает некоторые из возможных применений ИИ в борьбе с коррупцией:

— *государственные закупки:* контроль публичных тендеров путем мониторинга тендеров с целью выявления аномальных закономерностей, таких как индивидуальные тендеры или тендеры, в которых всегда выигрывает одна и та же компания. Проверка государственных контрактов на предмет наличия необычных положений или потенциально коррупционных условий;

— *публичные аудиты:* бюджетный аудит для анализа расходов муниципалитетов и других государственных администраций, выявления нерегулярных ассигнований или необоснованных расходов. Контроль субсидий и государственной помощи с целью выявления дублирования или несоответствия получателей;

— *обнаружение шаблонов:* обнаружение аномальных закономерностей с помощью машинного обучения, поскольку большие объемы данных могут быть проанализированы на предмет аномальных закономерностей, которые могут указывать на мошенническую деятельность. Например, в финансовых транзакциях, тендерах, контрактах или грантах. Анализ текста при проверке документов и электронных писем на предмет подозрительных терминов или закономерностей, например, в случае ложных сообщений;

— *человеческие ресурсы:* управление человеческими ресурсами для выявления нарушений в процессах отбора, внутренних продвижениях, обменах и т. д. Контроль конфликтов интересов путем выявления возможных взаимосвязей между сотрудниками органов государственного управления и частными компаниями;

— *коммунальные услуги:* выявление нарушений в управлении государственными услугами путем определения возможных перерасходов средств, недостатков или недобросовестной практики. Проверка официальных документов, проверка подлинности и соответствия документов, представляемых в административных процедурах, предотвращение подделок;

— *анализ данных:* интеграция баз данных — благодаря подключению общедоступных баз данных (местных, национальных или международных) можно создавать перекрестные ссылки на информацию и эффективнее выявлять возможные случаи мошенничества;

— *защита данных:* защита конфиденциальных данных путем оповещения о несанкционированном доступе или манипулировании го-

сударственными базами данных. Оптимизация расследований, поскольку при обнаружении возможного случая мошенничества ИИ может рекомендовать ряд шагов или действий на основе предыдущих случаев, тем самым оптимизируя ресурсы и время расследования;

— *информационные системы:* системы информирования о нарушениях — анонимные платформы информирования на базе искусственного интеллекта, обеспечивающие защиту осведомителей и достоверность полученной информации;

— *прогностические системы*: ИИ может помочь прогнозировать области или секторы с более высоким риском мошенничества в будущем на основе исторических данных и текущих тенденций;

— *обучение этике и общественной добросовестности:* для сотрудников органов государственного управления и граждан, адаптация их содержания к реальным потребностям каждого человека;

— *законодательство и прозрачность:* прозрачность в принятии решений — инструменты ИИ, которые объясняют, как принимаются определенные государственные или корпоративные решения, снижая вероятность неправомерного фаворитизма. Обзор законодательства и нормативных актов — ИИ может анализировать и сравнивать законодательство разных регионов или стран, чтобы предлагать изменения, которые уменьшат юридические пробелы, способствующие коррупции.

§ 2. Инструменты искусственного интеллекта, применяемые для борьбы с коррупцией

В сфере противодействия мошенничеству и коррупции уже применяются инструменты и приложения на основе ИИ. А. Лопес Асера приводит, в частности, такие примеры, сгруппировав их по преследуемым целям.

VigIA — инструмент ИИ для выявления коррупции в государственных закупках, разработанный Tic Tank Университета Росарио (Аргентина) при поддержке Банка развития Латинской Америки и Карибского бассейна для Окружного управления по надзору Боготы. Цель VigIA — выявлять контракты мэрии Боготы с высоким риском коррупции и неэффективности, используя данные, предоставляемые Электронной системой государственных закупок.

Percephtor — инструмент ИИ, разработанный мексиканской компанией для помощи гражданам в контроле за общественными работами, оценке эффективности работы политиков и борьбе с коррупцией. Распознает объекты по изображениям и видео. В 2022 г. было установлено, что правительство Мексики тратило в среднем 2,7 млн песо в минуту на общественные работы. Этот факт был раскрыт организацией «Мексиканцы против коррупции и безнаказанности», которая ссылается на незадекларированные расходы на CompraNet, портале, предназначенном для демонстрации государственных контрактов.

Проект Европейского союза *Digiwhist* — инструмент анализа больших данных, созданный для выявления мошенничества в государственных закупках на европейском уровне. Проект обрабатывает показатели и общедоступные данные и тесно сотрудничает с организациями, специализирующимися на раскрытии случаев коррупции. Digiwhist — это совместный проект шести европейских организаций под руководством Кембриджского университета. Для его реализации они изучили данные о государственных закупках из 35 юрисдикций, на основе которых была создана общедоступная база данных. На основе собранной информации Digiwhist разработал инструменты для повышения прозрачности и справедливости государственных закупок. Эти инструменты находятся в свободном доступе и представляют собой ценный ресурс для НКО, журналистов, государственных органов и бизнеса.

Европейские механизмы публичной подотчетности *(EuroPAM)* — инструмент ИИ, который позволяет сравнивать правовые и нормативные стандарты в различных юрисдикциях.

Европейский мониторинг тендеров *(MET)* — программное обеспечение для оценки рисков в процедурах государственных закупок.

В Великобритании примером уже разработанного и доказавшего свою эффективность инструмента является *Ravn* — программное обеспечение с ИИ, способное быстро и без ошибок фильтровать, индексировать и обобщать документы, превосходя по эффективности человека. Ravn получил известность благодаря своей роли в раскрытии дела о коррупции в Rolls-Royce в 2008 г., когда он помог британскому Управлению по борьбе с крупным мошенничеством (SFO) проанализировать 30 млн документов, обрабатывая 600 тыс. документов ежедневно.

Аналогичным образом в Испании налоговая администрация и органы социального обеспечения используют цифровые платформы, которые упрощают и автоматизируют процессы и, сопоставляя информацию, позволяют выявлять случаи мошенничества. С 2015 г. Главное управление инспекции труда и социального обеспечения использует программное обеспечение на основе искусственного интеллекта (ана-

лиз данных) для более гибкого выявления случаев мошенничества под названием «Инструмент борьбы с мошенничеством».

Налоговая администрация также располагает инструментом, с помощью которого автоматически проверяются представленные налогоплательщиками данные самооценки для выявления расхождений между данными, включенными в самооценку, и другими данными, имеющимися в распоряжении Казначейства.

Инструменты ИИ для обнаружения ложных сообщений. Испанская Национальная полиция уже использует систему искусственного интеллекта *VeriPol,* которая применяется для выявления ложных заявлений. Эта система была разработана совместно с Автономным университетом Мадрида в связи с ростом числа ложных заявлений о насильственных ограблениях. Система анализирует язык заявлений, используя методы обработки естественного языка и машинного обучения, и ее эффективность составляет 91%.

Инструменты ИИ для выявления случаев конфликта интересов. Искусственный интеллект может помочь в борьбе с коррупцией, выявляя нарушения и конфликты интересов посредством анализа больших объемов данных. Для эффективности ИИ крайне важно наличие точных алгоритмов и качественных данных, таких как *Arachne.*

Arachne — это цифровая система, созданная Европейской комиссией для улучшения контроля над проектами, финансируемыми структурными фондами ЕС, такими как Европейский социальный фонд (ESF) и Европейский фонд регионального развития (ERDF). Храня данные по этим проектам и используя общедоступную информацию, Arachne выявляет потенциальные риски мошенничества, конфликта интересов и нарушений. Однако она не предназначена для индивидуальной оценки бенефициаров или их автоматического исключения.

Данные о проектах поступают от управляющих органов ESF и ERDF. Arachne также использует информацию из внешних источников, таких как Orbis и World Compliance, для улучшения анализа. Инструмент рассчитывает специфические индикаторы риска.

Arachne собирает данные о бенефициарах, партнерах по проектам, подрядчиках, поставщиках услуг и других лицах, включая имена и адреса, а также данные о компаниях, акционерах и санкционных списках.

Arachne с ее методами анализа является важнейшим инструментом для управления органами власти в борьбе с мошенничеством и в совершенствовании управления проектами, финансируемыми ЕС.

Инструменты ИИ для предотвращения коррупции. В Венгрии для мониторинга государственных закупок создан *Red Flags,* финансируемый Европейской комиссией. Этот инструмент анализирует процедуры закупок и с помощью алгоритма определяет те из них, которые представляют наибольший риск коррупции, на основе предустановленных предупреждений в зависимости от их серьезности или вероятности обнаружения фактической коррупции. Кроме того, он предоставляет доступ к этой информации как гражданам, так и государственным служащим.

Служба социального обеспечения Испании использует алгоритм искусственного интеллекта для мониторинга сотрудников, находящихся на больничном, и выявления возможного мошенничества, включенный в проект LINCÉ. Этот инструмент прогнозирования оценивает состояние здоровья людей и прогнозирует вероятность их готовности вернуться к работе. Алгоритм определяет, какие документы должны быть рассмотрены медицинскими инспекторами Национального института социального обеспечения (INSS) в первую очередь, выявляет потенциальные случаи мошенничества.

Профессора Итурриага и Санс из Университета Вальядолида провели исследование, в котором использовали ИИ для прогнозирования того, в каких провинциях Испании уровень коррупции может возрасти в ближайшие годы. В исследовании, проведенном с использованием нейросети, были обработаны экономические и политические данные за период с 2000 по 2012 г. для выявления областей, подверженных коррупции, и условий, способствующих ей. Один из выводов заключается в том, что вероятность коррупции возрастает, если политическая партия находится у власти длительное время. Кроме того, такие факторы, как повышение налога на имущество, рост цен на жилье, открытие большого количества банковских отделений и создание новых компаний, могут указывать на наличие коррупции. Инновационность данного исследования заключается в использовании реальных данных, а не субъективных индексов восприятия, как это делалось ранее.

Проблемы, которые может вызвать внедрение ИИ. Внедрение инструментов ИИ в борьбу с мошенничеством и коррупцией может привести к возникновению следующих проблем:

— *проблемы с данными:* способность ИИ обнаруживать коррупцию зависит от качества, полноты и надежности данных — как данных, используемых для обучения системы, так и данных, которые система анализирует. Если данные неполные, предвзятые или устаревшие, то результаты, сгенерированные ИИ, будут отражать эти искажения и мо-

гут привести к неточным результатам, подрывая целостность антикоррупционных усилий. Например, проект MARA в Бразилии, который рассчитывает баллы коррупции с использованием данных о судимостях, страдает от политических предубеждений, которые формируют его обучающие наборы данных. Аналогичным образом, исследование систем ИИ, используемых для обнаружения отмывания денег, показало, что низкое качество данных приводит к значительному снижению точности;

— *сопротивление изменениям и отсутствие обучения*: одним из основных препятствий на пути внедрения ИИ является сопротивление изменениям со стороны сотрудников органов государственного управления. Многие специалисты могут ощущать угрозу вторжения технологий, которые, по их мнению, могут заменить их должности или помешать их привычной работе из-за отсутствия специальной подготовки по использованию этих инструментов.

Чтобы преодолеть это препятствие, крайне важно продвигать программы обучения и повышения квалификации, которые позволят сотрудникам лучше понимать ИИ, принципы его работы и то, как он может стать дополнительным инструментом, облегчающим и улучшающим их работу, а не заменяющим ее. Также крайне важно правильно управлять ожиданиями и четко доносить до сотрудников цели и преимущества этих инициатив;

— *вопросы конфиденциальности и защиты данных:* ИИ для его корректной работы необходим доступ к большим объемам данных. Однако управление этими данными в публичной сфере вызывает серьезные опасения относительно конфиденциальности и защиты персональных данных граждан. Неправомерное использование или непреднамеренное раскрытие этих данных может иметь серьезные последствия, особенно в случае осведомителей. Поэтому крайне важно разработать протоколы безопасности, которые обеспечат соответствие решений ИИ действующим правилам защиты данных;

— *отсутствие технологической инфраструктуры:* внедрение систем на основе ИИ требует развитой и современной технологической инфраструктуры. Поэтому крайне важно создавать совместные сети, а также привлекать национальные и европейские органы, продвигающие этот тип технологий;

— *отсутствие прозрачности и объяснимости:* многие системы ИИ работают как черные ящики, где процессы принятия решений непрозрачны, что затрудняет интерпретацию и проверку их результатов. Например, *проект Zero Trust в Китае* был направлен на выявление коррупции среди более чем 60 млн государственных служащих путем перекрестных ссылок на 150 баз данных, включая банковские выписки, данные о передаче имущества и частных покупках. Несмотря на эффективность в выявлении нарушений, которые могут указывать на коррупцию, внутренние исследователи признали неспособность системы объяснить, как она пришла к конкретным выводам. Государственным учреждениям может быть сложно предоставлять содержательные объяснения решений, принятых с помощью ИИ, что может подорвать принципы прозрачности и подотчетности в процессе принятия государственных решений. Такое отсутствие объяснимости подрывает доверие к выводам, принятым с помощью ИИ, в юридических контекстах, где доказательства должны соответствовать высоким стандартам доказывания и прозрачности.

Для снижения этого риска крайне важно применять критический и непрерывный подход к проверке и валидации моделей ИИ. Кроме того, необходимо разработать протоколы, позволяющие быстро исправлять ошибки и гарантировать, что системы не будут способствовать сохранению или усилению существующих предубеждений в данных или в обществе, а также обеспечить защиту основных прав граждан и конфиденциальности при использовании больших данных и автоматизированных систем органами государственного управления.

К. Рандиери, профессор Университета eCampus, директор Kwaai EMEA, основатель Intellisystem Technologies в статье в Forbes «Предвзятость и коррупция в сфере искусственного интеллекта: угроза справедливости» (14 марта 2025 г.) пишет: «Предвзятость моделей ИИ и возможность преднамеренного манипулирования поднимают множество этических и стратегических вопросов перед компаниями и институтами, призванными анализировать корни этих проблем, их последствия и стратегии смягчения их последствий».

В стандартной литературе когнитивное искажение определяется как систематическое искажение, влияющее на процессы принятия решений и когнитивное понимание, часто являющееся результатом ограниченности наборов данных, неосознанных предубеждений и протоколов принятия решений, благоприятствующих определенным точкам зрения. Однако предубеждение — это человеческий фактор, обусловленный внутренней характеристикой обработки информации нашим мозгом, часто возникающей в результате когнитивных сокращений, которые помогают нам принимать решения в кратчайшие сроки. Оно возникает всякий раз, когда человек пытается оценить текущую ситуацию, основываясь на своем прошлом опыте, по возможности опу-

ская различия, чтобы повторно использовать те же критерии, принятые в аналогичной ситуации. Однако игнорирование таких различий иногда может иметь решающее значение для аннулирования окончательной оценки, что может привести к систематическим искажениям в рассуждениях, влияющим на принимаемые решения. Системы ИИ становятся предвзятыми, когда модель обучается на асимметричных данных или когда в дизайне присутствуют структурные дефекты, что приводит к несправедливым результатам.

Эта проблема выходит за рамки одних лишь технологий и становится серьезным вопросом социальной справедливости и инклюзивности. Алгоритмическая предвзятость — серьезная проблема, возникающая из-за решений, принимаемых при создании алгоритма, независимо от того, были ли они преднамеренными или нет. Она может иметь очень серьезные последствия в таких областях, как выдача кредитов, найм персонала и система уголовного правосудия.

От проблем, возникающих из-за непреднамеренных последствий и результатов внедрения ИИ, следует отличать коррупционное использование ИИ — преднамеренное злоупотребление системами ИИ в целях личной выгоды преступников.

Наибольшую опасность среди методов манипуляции, обычно используемых в системах ИИ, представляет отравление данных, поскольку этот метод позволяет пользователям вставлять ложную информацию в обучающие наборы данных, что приводит к изменению поведения алгоритма и приоритетному решению лишь некоторых из проблем.

Уязвимости, основанные на моделях, известные как бэкдоры (англ. back door — задняя дверь), позволяют злоумышленникам контролировать алгоритмические решения, что создает значительные риски в таких областях, как безопасность и правосудие. Системы сталкиваются с манипуляцией входными данными посредством состязательных атак, что приводит к генерации неверных результатов при попытке обойти средства обнаружения мошенничества.

Коррупция в модели достигает своего разрушительного эффекта, когда кто-то изменяет ее основные параметры. Это создает кризис доверия к ИИ и приводит к этическим и эксплуатационным проблемам, требующим инновационных решений. Выявление этих проблем крайне важно для обеспечения справедливости и надежности систем ИИ.

Вмешательство в систему ИИ может быть вызвано разными причинами, такими как экономическая, политическая или даже неявная предвзятость, которую люди могут не до конца осознавать. Например,

в сфере финансовых услуг ИИ может использоваться для манипулирования рынком с помощью высокочастотных торговых алгоритмов или для того, чтобы дать другим инвесторам пищу для размышлений о ценах акций. В страховой отрасли, например, предвзятые алгоритмы ИИ могут отказать в страховании людям, считающимся подверженными высокому риску, что наносит ущерб так называемым маргинализированным группам.

С политической точки зрения, злоупотребление ИИ может повлиять на любую платформу, предназначенную для управления информацией в Интернете.

Рандиери считает, для того «чтобы искусственный интеллект продолжал оставаться инструментом справедливого и инклюзивного прогресса, необходимо принять стратегии смягчения последствий, включая повышение прозрачности процессов разработки, диверсификацию наборов данных, проведение независимых аудитов и внедрение специальных правил, эффективно предотвращающих злоупотребление этой технологией.

Только при глубокой коллективной приверженности компаний, правительств и гражданского общества станет возможным гарантировать, что такой мощный и распространенный инструмент, как ИИ, продолжит утверждать себя в качестве двигателя инноваций, не ставя под угрозу высшие человеческие ценности справедливости и равенства».

§ 3. Борьба с коррупцией с помощью искусственного интеллекта в Китае

Китай одним из первых в мире начал использовать ИИ для контроля за банковскими транзакциями. Одна из таких систем — *Zero Trust*. Она анализировала огромные объемы финансовых данных, подозрительные переводы, резкие изменения в доходах и необычную активность на счетах. Одновременно система изучала поведение людей в социальных сетях — например, неожиданные покупки, связь с известными коррупционерами или признаки роскошного образа жизни, которые не соответствуют официальным доходам. При обнаружении подозрительных схем Zero Trust автоматически отправляла сигнал правоохранительным органам.

В настоящее время вся антикоррупционная кампания в Китае основана на искусственном интеллекте и возглавляется такими инструментами, как *DeepSeek*.

Так, в марте 2025 г. Комиссия по проверке дисциплины и надзору муниципалитета Суйхуа провинции Хэйлунцзян сделала поразительное открытие. Используя большую языковую модель (LLM) DeepSeek для анализа данных о пособиях по старости, следователи выявили сеть мошеннических заявлений, связанных с «зомби-аккаунтами» — тремя умершими людьми, которые продолжали получать государственные субсидии. За фальсифицированными заявлениями скрывалась целая сеть коррупции, раскрывающая сговор как внутри, так и за пределами государственной службы.

Этот реальный случай знаменует начало новой эры борьбы с коррупцией с помощью ИИ в Китае.

Китай сталкивается с новыми вызовами государственного управления, поскольку традиционные системы надзора не успевают за изощренными злоупотреблениями. Среди основных новых форм коррупции — отмывание денег через виртуальные валюты, использование сложной структуры капитала для сокрытия незаконной деятельности и совмещение должностных обязанностей с незаконной деятельностью. Однако инструменты на базе ИИ, такие как DeepSeek, теперь демонстрируют способность раскрывать эти схемы гораздо быстрее, чем ручные расследования. Примером может служить случай, когда DeepSeek всего за 72 часа выявил сеть взяточничества, проходившую через 20 подставных компаний. Вручную раскрытие такого акта коррупции заняло бы три месяца.

Традиционные надзорные органы сталкиваются с такими проблемами, как информационная перегрузка, когнитивные слепые зоны и медленное реагирование. Появление решений на основе ИИ помогает решать эти проблемы благодаря передовым инструментам, таким как картирование взаимосвязей, мультимодальный когнитивный анализ и динамическое моделирование рисков, — все они меняют систему управления и надзора в КНР в таких областях, как социальное обеспечение, политический надзор и расследования.

Борьба с коррупцией в Китае с помощью ИИ произвела революцию в методах борьбы правительства с противоправными действиями. Более быстрое и эффективное выявление фактов коррупции потенциально сокращает время расследования с месяцев до нескольких дней; ИИ также усиливает контроль в таких областях, как социальное обеспечение, политический надзор и сбор доказательств.

Эта трансформация представляет собой сдвиг в системе государственного управления. Сочетание ИИ с политическими и правовыми нормами позволяет китайскому правительству создавать более эффективную и сложную систему борьбы с коррупцией. Однако, хотя ИИ и усиливает эффективность правоприменения, баланс между технологическим прогрессом и политической подотчетностью остается критически важным, учитывая авторитарные нормы, лежащие в основе китайской модели государственного управления.

С 2012 г. антикоррупционная кампания председателя Си Цзиньпина привела к расследованию и дисциплинарным мерам в отношении миллионов лиц, включая высокопоставленных деятелей. Кроме того, международные операции Пекина, такие как Fox Hunt, являющиеся частью его антикоррупционной кампании Skynet, привели к аресту и экстрадиции тысяч беглецов и возврату миллиардов незаконно выведенных средств. Национальная надзорная комиссия, созданная в 2018 г., усилила надзор за членами партии и государственными служащими. Высшие прокуроры Китая активизировали усилия по борьбе с коррупцией на низовом уровне, особенно в здравоохранении, образовании и занятости, поскольку эти сферы напрямую влияют на повседневную жизнь людей.

Несмотря на эти меры, коррупция остается глубоко укоренившейся. Многие аналитики утверждают, что системные реформы, помимо широкомасштабных репрессий, необходимы для долгосрочного прогресса. Китай занял 76-е место из 180 в Индексе восприятия коррупции (ИВК) Transparency International за 2024 г., набрав 43 балла. Коррупция особенно распространена в сферах недвижимости, строительства и сбора налогов.

По данным газеты South China Morning Post, антикоррупционная кампания в КНР активизировалась с 2024 г.: под следствие попали 56 высокопоставленных чиновников, что на 25% больше, чем в 2023 г. В целом, Центральная комиссия по проверке дисциплины расширила сферу своей деятельности, сосредоточившись на центральных ведомствах, государственных предприятиях и армии, стремясь искоренить коррупцию на высших уровнях власти.

В государственных предприятиях резко возросло число случаев коррупции: в 2024 г. расследование проводилось в отношении шести руководителей. Особенно пострадали авиационная и оборонная отрасли: под следствием находятся десятки руководителей высшего звена, включая Тань Жуйсуна, бывшего председателя Китайской корпорации авиационной промышленности. Репрессии распространились и на нефинансовые государственные предприятия, поскольку власти стремятся усилить контроль над стратегическими отраслями.

Народно-освободительная армия Китая (НОАК) также находится под все более пристальным вниманием, причем особое внимание уделяется Ракетным войскам НОАК, которые контролируют ядерный арсенал КНР. В опубликованном в марте 2025 г. ежегодном отчете о работе правительства Китая обсуждались укоренившиеся проблемы с коррупцией в армии и содержался призыв к «углублению политической санации» в оборонном секторе. Политическое падение нескольких высокопоставленных чиновников, включая бывших министров обороны Ли Шанфу и Вэй Фэнхэ, и отстранение от должности члена Центрального военного совета Мяо Хуа подчеркивают, насколько важна борьба с коррупцией для восстановления политического контроля Си Цзиньпина, поскольку речь идет о дисциплине.

Рост числа случаев коррупции в высших органах и министерствах Коммунистической партии за последние два года подкрепляет директиву Си Цзиньпина по искоренению взяточничества в секторах с высокой концентрацией власти и ресурсов. Бывший министр юстиции Тан Ицзюнь, министр сельского хозяйства Тан Жэньцзянь и руководитель национального спорта Гоу Чжунвэнь — вот лишь некоторые из видных деятелей, столкнувшихся с обвинениями в политической нелояльности, а также в коррупции.

Интеграция ИИ в систему государственного управления в КНР, особенно в рамках борьбы с коррупцией, вновь поднимает вопросы о прозрачности, этичном надзоре и конфиденциальности данных. Баланс между государственным контролем и прозрачностью ИИ представляет собой серьезную проблему, как и обеспечение беспристрастности алгоритмов.

Приложения

Приложение 1

Конвенция против киберпреступности; укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям, одобренная Генеральной Ассамблеей ООН 24 декабря 2024 г.

Преамбула

Государства — участники настоящей Конвенции,

принимая во внимание цели и принципы, провозглашенные в Уставе Организации Объединенных Наций,

отмечая, что информационно-коммуникационные технологии, обладая огромным потенциалом, способным содействовать развитию общества, открывают новые возможности для преступников, могут способствовать увеличению масштабов и разнообразия преступной деятельности и иметь негативные последствия для государств, предприятий и благополучия людей и общества в целом,

будучи обеспокоены тем, что использование информационно-коммуникационных систем может оказывать значительное влияние на масштабы, скорость совершения и объем уголовных правонарушений, включая правонарушения, связанные с терроризмом и транснациональной организованной преступностью, такие как торговля людьми, незаконный ввоз мигрантов, незаконное изготовление и оборот огнестрельного оружия, его составных частей, компонентов и боеприпасов к нему, незаконный оборот наркотиков и незаконный оборот культурных ценностей,

будучи убеждены в необходимости в первоочередном порядке осуществлять глобальную политику в области уголовного правосудия, направленную на защиту общества от киберпреступности, путем, в частности, принятия соответствующего законодательства, установле-

ния общих составов преступлений и процессуальных полномочий и укрепления международного сотрудничества в целях более эффективного предупреждения такой деятельности и противодействия ей на национальном, региональном и международном уровнях,

будучи исполнены решимости лишать безопасного убежища тех, кто вовлечен в киберпреступность, путем уголовного преследования за эти преступления, где бы они ни совершались,

подчеркивая необходимость расширения координации и сотрудничества между государствами, в частности путем оказания технической помощи и укрепления потенциала, включая передачу технологий на взаимно согласованных условиях, странам, в особенности развивающимся странам, по их просьбе, в целях совершенствования внутреннего законодательства и правовых норм и наращивания потенциала национальных органов для противодействия киберпреступности во всех ее формах, в том числе посредством предупреждения, выявления и расследования преступлений и уголовного преследования за них, и особо отмечая в этой связи роль Организации Объединенных Наций,

признавая рост числа жертв киберпреступности, важность обеспечения правосудия для этих жертв и необходимость учета потребностей лиц, находящихся в уязвимом положении, при осуществлении мер по предупреждению преступлений, охватываемых настоящей Конвенцией, и борьбе с ними,

будучи исполнены решимости более эффективно предупреждать, выявлять и пресекать международные переводы имущества, полученного в результате киберпреступлений, и укреплять международное сотрудничество в вопросах изъятия и возвращения доходов от преступлений, признанных таковыми в соответствии с настоящей Конвенцией,

принимая во внимание, что предупреждение киберпреступности и борьба с ней — это обязанность всех государств и что для обеспечения эффективности своих усилий в данной области они должны сотрудничать друг с другом при поддержке и участии соответствующих международных и региональных организаций, а также неправительственных организаций, организаций гражданского общества, научных учреждений и структур частного сектора,

признавая важность учета гендерных факторов во всей соответствующей деятельности по предупреждению преступлений, охватываемых настоящей Конвенцией, и борьбе с ними в соответствии с внутренним законодательством, учитывая необходимость решения задач правоприменения и обеспечения уважения прав человека и основных

свобод, закрепленных в применимых международных и региональных документах,

признавая право на защиту от произвольного или незаконного вмешательства в частную жизнь людей и важность защиты персональных данных,

высоко оценивая работу Управления Организации Объединенных Наций по наркотикам и преступности и других международных и региональных организаций по предупреждению киберпреступности и борьбе с ней,

ссылаясь на резолюции Генеральной Ассамблеи 74/247 от 27 декабря 2019 года и 75/282 от 26 мая 2021 года,

принимая во внимание существующие международные и региональные конвенции и договоры о сотрудничестве в уголовно-правовых вопросах, а также аналогичные договоры, существующие между государствами — членами Организации Объединенных Наций, согласились о нижеследующем:

Глава I. Общие положения

Статья 1. Цели

Целями настоящей Конвенции являются:

a) содействие принятию и укрепление мер, направленных на повышение эффективности и результативности предупреждения киберпреступности и борьбы с ней;

b) поощрение, облегчение и укрепление международного сотрудничества в предупреждении киберпреступности и борьбе с ней; и

c) поощрение, облегчение и поддержка технической помощи и создания потенциала в целях предупреждения киберпреступности и борьбы с ней, особенно в интересах развивающихся стран.

Статья 2. Термины

Для целей настоящей Конвенции:

a) «информационно-коммуникационная система» означает любое устройство или группу соединенных или взаимосвязанных устройств, одно или несколько из которых по команде программы производит сбор, хранение и автоматическую обработку электронных данных;

b) «электронные данные» означают любое представление фактов, информации или концепций в форме, пригодной для обработки в информационно-коммуникационной системе, включая соответствую-

щую программу, в результате действия которой информационно-коммуникационная система выполняет ту или иную функцию;

c) «данные о трафике» означают любые электронные данные, относящиеся к сообщению, осуществляемому посредством информационно-коммуникационной системы, генерируемые информационно-коммуникационной системой, являвшейся составной частью коммуникационной цепочки, которые указывают на источник, адресата, маршрут, время, дату, размер и продолжительность сообщения или тип соответствующей услуги;

d) «данные о содержании» означают любые электронные данные, помимо абонентских данных и данных о трафике, относящиеся к содержанию данных, переданных посредством информационно-коммуникационной системы, включая, в частности, изображения, текстовые сообщения, голосовые сообщения, аудиозапись и видеозапись;

e) «поставщик услуг» означает любую государственную или частную структуру, которая:

i) обеспечивает пользователям ее услуг возможность обмена информацией посредством использования информационно-коммуникационной системы или

ii) осуществляет обработку или хранение электронных данных от имени такого поставщика коммуникационных услуг или пользователей таких услуг;

f) «абонентские данные» означают любые имеющиеся у поставщика услуг сведения о его абонентах, кроме данных о трафике или содержании, с помощью которых можно определить:

i) вид используемой коммуникационной услуги, принятые в связи с ней меры технического обеспечения и период оказания услуги;

ii) личность абонента, его почтовый или географический адрес, номер телефона или другого средства связи, расчетные или платежные реквизиты, имеющиеся на основании соглашения или договоренности об обслуживании;

iii) любые другие сведения о месте установки коммуникационного оборудования, имеющиеся на основании соглашения или договоренности об обслуживании;

g) «персональные данные» означают любую информацию, относящуюся к определенному или определяемому физическому лицу;

h) «серьезное преступление» означает преступление, наказуемое лишением свободы на максимальный срок не менее четырех лет или более строгой мерой наказания;

i) «имущество» означает любые активы, будь то материальные или нематериальные, движимые или недвижимые, выраженные в вещах или в правах, включая виртуальные активы, а также юридические документы или акты, подтверждающие право на такие активы или интерес в них;

j) «доходы от преступления» означают любое имущество, приобретенное или полученное, прямо или косвенно, в результате совершения какого-либо преступления;

k) «замораживание» или «арест» означает временное запрещение передачи, преобразования, отчуждения или передвижения имущества либо временное осуществление его хранения или контроля над ним по постановлению суда или другого компетентного органа;

l) «конфискация» означает окончательное лишение имущества по постановлению суда или другого компетентного органа;

m) «основное преступление» означает любое преступление, в результате которого были получены доходы, в отношении которых могут быть совершены преступления, указанные в статье 17 настоящей Конвенции;

n) «региональная организация экономической интеграции» означает организацию, созданную суверенными государствами какого-либо региона, которой ее государства-члены передали полномочия по вопросам, регулируемым настоящей Конвенцией, и которая должным образом уполномочена в соответствии с ее внутренними процедурами подписывать, ратифицировать, принимать, утверждать настоящую Конвенцию или присоединяться к ней; ссылки в настоящей Конвенции на «Государства-участники» относятся к таким организациям в пределах их компетенции;

o) «чрезвычайная ситуация» означает ситуацию, в которой существует значительный и неизбежный риск для жизни или безопасности любого физического лица.

Статья 3. Сфера применения

Настоящая Конвенция, если в ней не указано иное, применяется:

a) к предупреждению и расследованию уголовных правонарушений, признанных таковыми в соответствии с настоящей Конвенцией, и преследованию за них, включая замораживание, арест, конфискацию и возвращение доходов от таких правонарушений;

b) к сбору, получению, сохранению и передаче доказательств в электронной форме для целей уголовного расследования или судопроизводства, как это предусмотрено в статьях 23 и 35 настоящей Конвенции.

Статья 4. Преступления, признанные таковыми в соответствии с другими конвенциями и протоколами Организации Объединенных Наций

1. При осуществлении других применимых конвенций и протоколов Организации Объединенных Наций, участниками которых являются государства-участники, они обеспечивают, чтобы уголовные правонарушения, признанные таковыми в соответствии с этими конвенциями и протоколами, также считались уголовными правонарушениями по внутреннему законодательству, если они совершаются с использованием информационно-коммуникационных систем.

2. Ничто в настоящей статье не должно толковаться как признание деяний уголовно наказуемыми в соответствии с настоящей Конвенцией.

Статья 5. Защита суверенитета

1. Государства-участники выполняют свои обязательства согласно настоящей Конвенции в соответствии с принципами суверенного равенства и территориальной целостности государств и принципом невмешательства во внутренние дела других государств.

2. Ничто в настоящей Конвенции не наделяет Государство-участника правом осуществлять на территории другого государства юрисдикцию и функции, которые входят исключительно в компетенцию органов этого другого государства в соответствии с его внутренним законодательством.

Статья 6. Соблюдение прав человека

1. Государства-участники обеспечивают, чтобы выполнение их обязательств, вытекающих из настоящей Конвенции, соответствовало их обязательствам по международному праву в области прав человека.

2. Ничто в настоящей Конвенции не толкуется как допускающее подавление прав человека или основных свобод, включая права, касающиеся свободы выражения, совести, мнений, религии или убеждений, мирных собраний и объединений, в соответствии и согласно с применимыми нормами международного права в области прав человека.

Глава II. Криминализация

Статья 7. Незаконный доступ

1. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться, с тем чтобы признать в соответствии со своим внутренним законодательством в качестве уголовного правонарушения, когда такое деяние совершается умышленно, неправомерный доступ к информационно-коммуникационной системе в целом или любой ее части.

2. Государство-участник может установить требование, чтобы правонарушение было совершено путем нарушения мер безопасности, с намерением получить электронные данные или с иным бесчестным или преступным умыслом либо в отношении информационно-коммуникационной системы, соединенной с другой информационно-коммуникационной системой.

Статья 8. Незаконный перехват

1. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться, с тем чтобы признать в соответствии со своим внутренним законодательством в качестве уголовного правонарушения, когда такое деяние совершается умышленно и неправомерно, осуществляемый с помощью технических средств перехват непубличных передач электронных данных в информационно-коммуникационную систему, из нее или внутри нее, в том числе электромагнитного излучения от информационно-коммуникационной системы, переносящего такие электронные данные.

2. Государство-участник может установить требование, чтобы правонарушение было совершено с бесчестным или преступным умыслом либо в отношении информационно-коммуникационной системы, соединенной с другой информационно-коммуникационной системой.

Статья 9. Воздействие на электронные данные

1. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться, с тем чтобы признать в соответствии со своим внутренним законодательством в качестве уголовных правонарушений, когда такие деяния совершаются умышленно и неправомерно, повреждение, удаление, порчу, изменение или блокирование электронных данных.

2. Государство-участник может установить требование, чтобы деяние, предусмотренное пунктом 1 настоящей статьи, влекло за собой серьезный ущерб.

Статья 10. Воздействие на информационно-коммуникационную систему

Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться, с тем чтобы признать в соответствии со своим внутренним законодательством в качестве уголовного правонарушения, когда такое деяние совершается умышленно и неправомерно, серьезное препятствование функционированию информационно-коммуникационной системы путем ввода, передачи, повреждения, удаления, порчи, изменения или блокирования электронных данных.

Статья 11. Неправомерное использование устройств

1. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться, с тем чтобы признать в соответствии со своим внутренним законодательством в качестве уголовных правонарушений, когда деяния совершаются умышленно и неправомерно:

a) получение, производство, продажу, приобретение для использования, ввоз, распространение или предоставление иным способом:

i) устройств, включая программное обеспечение, разработанных или адаптированных прежде всего для целей совершения какого-либо из преступлений, признанных таковыми в соответствии со статьями 7—10 настоящей Конвенции; или

ii) пароля, реквизитов доступа, электронной подписи или аналогичных данных, позволяющих получить доступ ко всей информационно-коммуникационной системе или любой ее части;

с намерением, чтобы устройство, включая программное обеспечение, или пароль, реквизиты доступа, электронная подпись или аналогичные данные были использованы в целях совершения любого из преступлений, признанных таковыми в соответствии со статьями 7—10 настоящей Конвенции; и

b) владение объектами, указанными в подпункте (i) или (ii) подпункта (a) пункта 1 настоящей статьи, с намерением, чтобы они были использованы для совершения любого из преступлений, признанных таковыми в соответствии со статьями 7—10 настоящей Конвенции.

2. Настоящая статья не толкуется как устанавливающая уголовную ответственность в тех случаях, когда получение, производство, продажа, приобретение для использования, ввоз, распространение или иная форма предоставления или владение, указанные в пункте 1 настоящей статьи, не преследуют цель совершения какого-либо из преступлений, признанных таковыми в соответствии со статьями 7—10 настоящей Конвенции, а связаны, например, с разрешенным испытанием или защитой информационно-коммуникационной системы.

3. Каждое Государство-участник может сохранить за собой право не применять положения пункта 1 настоящей статьи при условии, что такая оговорка не будет касаться продажи, распространения или иной формы предоставления объектов, указанных в подпункте (a)(ii) пункта 1 настоящей статьи.

Статья 12. Подлог с использованием информационно-коммуникационной системы

1. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться, с тем чтобы признать в соответствии со своим внутренним законодательством в качестве уголовных правонарушений, когда такие деяния совершаются умышленно и неправомерно, ввод, изменение, удаление или блокирование электронных данных, приводящие к возникновению неаутентичных данных, с намерением, чтобы они рассматривались или использовались в юридических целях в качестве аутентичных, независимо от того, поддаются ли эти данные непосредственному прочтению и являются ли они понятными.

2. Государство-участник может потребовать, чтобы условием наступления уголовной ответственности являлось наличие намерения совершить обман или аналогичного бесчестного или преступного умысла.

Статья 13. Хищение или мошенничество с использованием информационно-коммуникационной системы

Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться, с тем чтобы признать в соответствии со своим внутренним законодательством в качестве уголовного правонарушения, когда такое деяние совершается умышленно и неправомерно, лишение другого лица его собственности путем:

a) любого ввода, изменения, удаления или блокирования электронных данных;

b) любого вмешательства в функционирование информационно-коммуникационной системы;

c) любого обмана в отношении фактических обстоятельств, совершенного с использованием информационно-коммуникационной системы и побуждающего лицо к какому-либо действию или бездействию, которого это лицо в противном случае не совершило бы;

с мошенническим или бесчестным умыслом неправомерного извлечения для себя или для другого лица денежной или иной имущественной выгоды.

Статья 14. Преступления, связанные с размещением в Интернете материалов со сценами сексуальных надругательств над детьми или их сексуальной эксплуатации

1. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться, с тем чтобы признать в соответствии со своим внутренним законодательством в качестве уголовных правонарушений, когда такие деяния совершаются умышленно и неправомерно, следующие действия:

a) производство, предложение, продажу, распространение, передачу, транслирование, демонстрацию, публикацию или предоставление иным способом материалов со сценами сексуальных надругательств над детьми или их сексуальной эксплуатации, осуществляемые с помощью информационно-коммуникационной системы;

b) добывание или приобретение материалов со сценами сексуальных надругательств над детьми или их сексуальной эксплуатации либо получение доступа к таким материалам с помощью информационно-коммуникационной системы;

c) владение материалами со сценами сексуальных надругательств над детьми или их сексуальной эксплуатации, хранящимися в информационно-коммуникационной системе или на другом носителе информации, или контроль над такими материалами;

d) финансирование преступлений, признанных таковыми в соответствии с подпунктами (a)—(c) настоящего пункта, которое государства-участники могут признать отдельным преступлением.

2. Для целей настоящей статьи термин «материалы со сценами сексуальных надругательств над детьми или их сексуальной эксплуатации» включает визуальные материалы и может включать письменные или аудиоматериалы, изображающие, описывающие или представляющие любое лицо, не достигшее 18-летнего возраста:

a) которое реально совершает или имитирует сексуальные действия;

b) которое находится в присутствии человека, совершающего сексуальные действия;

c) интимные части тела которого демонстрируются главным образом в сексуальных целях или

d) которое подвергается пыткам или жестокому, бесчеловечному или унижающему достоинство обращению или наказанию, и такие материалы носят сексуальный характер.

3. Государство-участник может потребовать, чтобы к материалам, указанным в пункте 2 настоящей статьи, относились только материалы, которые:

a) изображают, описывают или представляют существующего человека или

b) визуально изображают акты сексуальных надругательств над ребенком или сексуальной эксплуатации ребенка.

4. Государства-участники могут в соответствии с внутренним законодательством и применимыми международными обязательствами принять меры, чтобы исключить криминализацию:

a) действий детей, самостоятельно создающих материалы, изображающие их; или

b) производства или передачи по взаимному согласию материалов, о которых идет речь в подпунктах (a)—(c) пункта 2 настоящей статьи, или владения ими по взаимному согласию, если изображенные в них действия законны согласно внутреннему законодательству и если такие материалы сохраняются исключительно для частного использования соответствующими лицами по взаимному согласию.

5. Ничто в настоящей Конвенции не затрагивает любые международные обязательства, которые в большей степени способствуют осуществлению прав ребенка.

Статья 15. Домогательство или создание доверительных отношений с целью совершения сексуального преступления в отношении ребенка

1. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться, с тем чтобы признать в соответствии со своим внутренним законодательством в качестве уголовных правонарушений умышленное общение с ребенком, домогательство его, создание доверительных отношений или вступление в

какие-либо договоренности с ним с помощью информационно-коммуникационной системы с целью совершения в отношении ребенка сексуального преступления, как оно определено во внутреннем законодательстве, в том числе любого из преступлений, признанных таковыми в соответствии со статьей 14 настоящей Конвенции.

2. Государство-участник может потребовать, чтобы состав преступления, указанного в пункте 1 настоящей статьи, включал определенные действия, направленные на его совершение.

3. Государство-участник может рассмотреть вопрос о распространении уголовной ответственности, предусмотренной в пункте 1 настоящей статьи, на действия в отношении лица, принимаемого за ребенка.

4. Государства-участники могут принять меры, чтобы исключить криминализацию действий, указанных в пункте 1 настоящей статьи, если они совершены детьми.

Статья 16. Распространение интимных изображений без согласия

1. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться, с тем чтобы признать в соответствии со своим внутренним законодательством в качестве уголовных правонарушений, когда такие деяния совершаются умышленно и неправомерно, продажу, распространение, передачу, публикацию или предоставление иным способом интимного изображения человека с помощью информационно-коммуникационной системы без согласия лица, представленного на этом изображении.

2. Для целей пункта 1 настоящей статьи «интимное изображение» означает визуальную запись сексуального характера с изображением человека старше 18 лет, произведенную любым способом, включая фотосъемку или видеозапись, на которой этот человек показан с обнаженными интимными частями тела или совершает сексуальные действия, которая в момент записи была конфиденциальной и в отношении которой у представленного на ней лица или лиц на момент, когда совершалось преступление, были разумные основания ожидать, что она останется конфиденциальной.

3. Государство-участник может в соответствующих случаях распространить определение интимного изображения на изображения лиц, не достигших 18-летнего возраста, если по внутреннему законодательству они достигли допустимого возраста вступления в сексуальные отношения и на изображении нет сцен надругательств над детьми или их эксплуатации.

4. Для целей настоящей статьи представленное на интимном изображении лицо, не достигшее 18-летнего возраста, не может давать согласие на распространение интимного изображения, которое в соответствии со статьей 14 настоящей Конвенции представляет собой материал со сценами сексуальных надругательств над детьми или их сексуальной эксплуатации.

5. Государство-участник может установить требование, чтобы условием наступления уголовной ответственности являлось наличие умысла причинить вред.

6. Государства-участники могут принимать другие меры по вопросам, касающимся настоящей статьи, в соответствии со своим внутренним законодательством и применимыми международными обязательствами.

Статья 17. Отмывание доходов от преступлений

1. Каждое Государство-участник принимает, в соответствии с основополагающими принципами своего внутреннего законодательства, такие законодательные и иные меры, какие могут потребоваться, с тем чтобы признать в качестве уголовных правонарушений следующие деяния, когда они совершаются умышленно:

a) i) преобразование или передачу имущества, если известно, что такое имущество представляет собой доходы от преступления, в целях сокрытия или утаивания преступного происхождения этого имущества или в целях оказания помощи любому лицу, участвующему в совершении основного преступления, с тем чтобы это лицо могло избежать правовых последствий своих действий;

ii) сокрытие или утаивание подлинного характера, источника, местонахождения, способа распоряжения, перемещения, прав на имущество или его принадлежности, если известно, что такое имущество представляет собой доходы от преступления;

b) при условии соблюдения основных принципов своей правовой системы:

i) приобретение имущества, владение им или его использование, если в момент его получения известно, что такое имущество представляет собой доходы от преступления;

ii) участие, объединение или вступление в сговор с целью совершения любого из преступлений, признанных таковыми в соответствии с на-

стоящей статьей, покушение на его совершение, а также пособничество, подстрекательство, содействие или дача советов для его совершения.

2. Для целей осуществления или применения пункта 1 настоящей статьи:

a) каждое Государство-участник включает в число основных преступлений соответствующие преступления, признанные таковыми в соответствии со статьями 7—16 настоящей Конвенции;

b) в случае, когда законодательство государств-участников содержит перечень конкретных основных преступлений, в него включается как минимум всеобъемлющий круг преступлений, признанных таковыми в соответствии со статьями 7—16 настоящей Конвенции;

c) для целей подпункта (b) настоящего пункта основные преступления включают преступления, совершенные как в пределах, так и за пределами юрисдикции соответствующего Государства-участника. Однако преступления, совершенные за пределами юрисдикции какого-либо Государства-участника, квалифицируются как основные преступления только при условии, что соответствующее деяние является уголовно наказуемым согласно внутреннему законодательству государства, в котором оно совершено, и было бы уголовно наказуемым согласно внутреннему законодательству Государства-участника, в котором осуществляется или применяется настоящая статья, если бы оно было совершено в нем;

d) каждое Государство-участник представляет Генеральному секретарю Организации Объединенных Наций тексты своих законов, обеспечивающих осуществление положений настоящей статьи, а также тексты любых последующих изменений к таким законам или их описание;

e) если этого требуют основополагающие принципы внутреннего законодательства Государства-участника, то можно предусмотреть, что преступления, указанные в пункте 1 настоящей статьи, не относятся к лицам, совершившим основное преступление;

f) осознание, умысел или цель как элементы состава преступления, указанного в пункте 1 настоящей статьи, могут быть установлены из объективных фактических обстоятельств дела.

Статья 18. Ответственность юридических лиц

1. Каждое Государство-участник принимает такие меры, какие с учетом его правовых принципов могут потребоваться для установления ответственности юридических лиц за участие в преступлениях, признанных таковыми в соответствии с настоящей Конвенцией.

2. В зависимости от правовых принципов Государства-участника ответственность юридических лиц может быть уголовной, гражданско-правовой или административной.

3. Такая ответственность действует без ущерба для уголовной ответственности физических лиц, совершивших преступления.

4. Каждое Государство-участник, в частности, обеспечивает применение в отношении юридических лиц, привлекаемых к ответственности в соответствии с настоящей статьей, эффективных, соразмерных и оказывающих сдерживающее воздействие уголовных или неуголовных санкций, включая денежные санкции.

Статья 19. Участие и покушение

1. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться, с тем чтобы признать в соответствии со своим внутренним законодательством в качестве уголовного правонарушения, когда такое деяние совершается умышленно, участие в любом качестве, например в качестве сообщника, пособника или подстрекателя, в совершении какого-либо преступления, признанного таковым в соответствии с настоящей Конвенцией.

2. Каждое Государство-участник может принять необходимые законодательные и иные меры, с тем чтобы признать в соответствии со своим внутренним законодательством в качестве уголовного правонарушения, когда такое деяние совершается умышленно, любое покушение на совершение какого-либо преступления, признанного таковым в соответствии с настоящей Конвенцией.

3. Каждое Государство-участник может принять необходимые законодательные и иные меры, с тем чтобы признать в соответствии со своим внутренним законодательством в качестве уголовного правонарушения, когда такое деяние совершается умышленно, приготовление к совершению какого-либо преступления, признанного таковым в соответствии с настоящей Конвенцией.

Статья 20. Срок давности

Каждое Государство-участник в надлежащих случаях с учетом тяжести преступления устанавливает согласно своему внутреннему законодательству длительный срок давности для возбуждения производства в отношении любого преступления, признанного таковым в соответствии с настоящей Конвенцией, и устанавливает более продолжительный срок давности или предусматривает возможность при-

остановления течения срока давности в тех случаях, когда лицо, предположительно совершившее преступление, уклоняется от правосудия.

Статья 21. Уголовное преследование, вынесение судебного решения и санкции

1. Каждое Государство-участник за совершение какого-либо преступления, признанного таковым в соответствии с настоящей Конвенцией, предусматривает применение эффективных, соразмерных и оказывающих сдерживающее воздействие санкций, учитывающих тяжесть преступления.

2. Каждое Государство-участник может принимать в соответствии со своим внутренним законодательством такие законодательные и иные меры, какие могут потребоваться для установления отягчающих обстоятельств преступлений, признанных таковыми в соответствии с настоящей Конвенцией, включая обстоятельства, затрагивающие критическую информационную инфраструктуру.

3. Каждое Государство-участник стремится обеспечить использование любых предусмотренных в его внутреннем законодательстве дискреционных юридических полномочий, относящихся к уголовному преследованию лиц за преступления, признанные таковыми в соответствии с настоящей Конвенцией, для достижения максимальной эффективности правоохранительных мер в отношении этих преступлений и с должным учетом необходимости воспрепятствовать совершению таких преступлений.

4. Каждое Государство-участник обеспечивает, чтобы любое лицо, преследуемое за преступления, признанные таковыми в соответствии с настоящей Конвенцией, пользовалось всеми правами и гарантиями согласно внутреннему законодательству и в соответствии с применимыми международными обязательствами Государства-участника, включая право на справедливое судебное разбирательство и права защиты.

5. Применительно к преступлениям, признанным таковыми в соответствии с настоящей Конвенцией, каждое Государство-участник принимает надлежащие меры, в соответствии со своим внутренним законодательством и с должным учетом прав защиты, в целях обеспечения того, чтобы условия, устанавливаемые в связи с решениями об освобождении до судебного разбирательства или окончания производства в связи с обжалованием, учитывали необходимость обеспечения присутствия обвиняемого в ходе последующего уголовного производства.

6. Каждое Государство-участник учитывает тяжесть соответствующих преступлений при рассмотрении вопроса о возможности досрочного или условного освобождения лиц, осужденных за такие преступления.

7. Государства-участники обеспечивают, чтобы во внутреннем законодательстве были предусмотрены надлежащие меры для защиты детей, обвиняемых в совершении преступлений, признанных таковыми в соответствии с настоящей Конвенцией, согласно обязательствам по Конвенции о правах ребенка и применимым протоколам к ней и другим применимым международным или региональным документам.

8. Ничто содержащееся в настоящей Конвенции не затрагивает принципа, согласно которому определение преступлений, признанных таковыми в соответствии с настоящей Конвенцией, и применимых юридических средств защиты или других правовых принципов, определяющих правомерность деяний, входит в сферу внутреннего законодательства каждого Государства-участника, а уголовное преследование и наказание за такие преступления осуществляются в соответствии с этим законодательством.

Глава III. Юрисдикция

Статья 22. Юрисдикция

1. 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:

a) преступление совершено на территории этого Государства-участника или

b) преступление совершено на борту судна, которое несло флаг этого Государства-участника в момент совершения преступления, или воздушного судна, которое зарегистрировано в соответствии с законодательством этого Государства-участника в такой момент.

2. При условии соблюдения статьи 5 настоящей Конвенции Государство-участник может также установить свою юрисдикцию в отношении любого такого преступления, когда:

a) преступление совершено против гражданина этого Государства-участника; или

b) преступление совершено гражданином этого Государства-участника или лицом без гражданства, которое обычно проживает на его территории; или

c) преступление является одним из преступлений, признанных таковыми в соответствии с подпунктом (b) (ii) пункта 1 статьи 17 настоящей Конвенции, и совершено за пределами его территории с целью совершения какого-либо преступления, признанного таковым в соответствии с подпунктом (i) или (ii) подпункта (a) или подпунктом (i) подпункта (b) пункта 1 статьи 17 настоящей Конвенции, на его территории; или

d) преступление совершено против этого Государства-участника.

3. Для целей пункта 11 статьи 37 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, предположительно совершившее преступление, находится на его территории и оно не выдает такое лицо лишь на том основании, что оно является одним из его граждан.

4. Каждое Государство-участник может также принять такие меры, какие могут потребоваться, с тем чтобы установить свою юрисдикцию в отношении преступлений, признанных таковыми в соответствии с настоящей Конвенцией, когда лицо, предположительно совершившее преступление, находится на его территории и оно не выдает его.

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 юрисдикции, установленной Государством-участником в соответствии со своим внутренним законодательством.

Глава IV. Процессуальные меры и правоприменение

Статья 23. Сфера применения процессуальных мер

1. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться для установления полномочий и процедур, предусмотренных в настоящей главе, в целях проведения конкретных уголовных расследований или судебных разбирательств.

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

a) уголовных правонарушений, признанных таковыми в соответствии с настоящей Конвенцией;

b) других уголовных правонарушений, совершенных с помощью информационно-коммуникационной системы; и

c) сбора доказательств в электронной форме, относящихся к любому уголовному правонарушению.

3. a) Каждое Государство-участник может сделать оговорку о сохранении за собой права применять меры, предусмотренные статьей 29 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 30 настоящей Конвенции. Каждое Государство-участник рассматривает возможность ограничения сферы действия такой оговорки в целях максимально широкого применения мер, указанных в статье 29.

b) Если Государство-участник ввиду ограничений, предусмотренных его внутренним законодательством, действующим на момент принятия настоящей Конвенции, не имеет возможности применить меры, указанные в статьях 29 и 30 настоящей Конвенции, в отношении сообщений, передаваемых внутри информационно-коммуникационной системы поставщика услуг, которая:

i) используется для обслуживания отдельной группы пользователей;

ii) не использует коммуникационные сети общего пользования и не соединена с другой информационно-коммуникационной системой, будь то общего доступа или частной;

это Государство-участник может сохранить за собой право не применять указанные меры к таким сообщениям. Каждое Государство-участник рассматривает возможность ограничения сферы действия такой оговорки в целях максимально широкого применения мер, указанных в статьях 29 и 30 настоящей Конвенции.

Статья 24. Условия и гарантии

1. Каждое Государство-участник обеспечивает, чтобы полномочия и процедуры, указанные в настоящей главе, устанавливались, осуществлялись и применялись в соответствии с условиями и гарантиями, предусмотренными в его внутреннем законодательстве, кото-

рые должны обеспечивать защиту прав человека в соответствии с его обязательствами по международному праву в области прав человека и включать в себя принцип соразмерности.

2. В соответствии и согласно с внутренним законодательством каждого Государства-участника такие условия и гарантии с учетом характера соответствующей процедуры или полномочий включают среди прочего судебную или иную независимую проверку, право на эффективное средство правовой защиты, основания правомочности применения и ограничение сферы и сроков действия такого полномочия или процедуры.

3. В той мере, в какой это соответствует общественным интересам, в частности интересам надлежащего отправления правосудия, каждое Государство-участник рассматривает влияние предусмотренных данной статьей полномочий и процедур на права, обязанности и законные интересы третьих сторон.

4. Условия и гарантии, установленные в соответствии с настоящей статьей, применяются на национальном уровне к полномочиям и процедурам, предусмотренным в настоящей главе, как для целей внутренних уголовных расследований и разбирательств, так и для целей международного сотрудничества со стороны запрашиваемого Государства-участника.

5. Под судебной или иной независимой проверкой, упомянутой в пункте 2 настоящей статьи, подразумевается проверка на национальном уровне.

Статья 25. Оперативное обеспечение сохранности хранимых электронных данных

1. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться, с тем чтобы его компетентные органы могли посредством дачи распоряжений или иным аналогичным образом оперативно обеспечивать сохранность конкретных электронных данных, включая данные о трафике, данные о содержании и абонентские данные, которые хранятся в информационно-коммуникационной системе, в частности когда имеются основания полагать, что эти электронные данные особенно подвержены риску утраты или изменения.

2. Если Государство-участник реализует положения пункта 1 настоящей статьи посредством дачи распоряжения какому-либо лицу об обеспечении сохранности конкретных хранимых электронных данных, которые находятся во владении или под контролем этого лица, то это Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться для того, чтобы обязать это лицо обеспечивать сохранность этих электронных данных и их целостность в течение необходимого периода времени, не превышающего 90 дней, с тем чтобы компетентные органы могли добиться их раскрытия. Государство-участник может предусмотреть возможность продления срока действия такого распоряжения.

3. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться, с тем чтобы обязать хранителя электронных данных или другое лицо, на которое возложено обеспечение их сохранности, соблюдать конфиденциальность выполнения таких процедур в течение срока, установленного в его внутреннем законодательстве.

Статья 26. Оперативное обеспечение сохранности и частичное раскрытие данных о трафике

Каждое Государство-участник принимает в отношении данных о трафике, сохранность которых требуется обеспечить в соответствии с положениями статьи 25 настоящей Конвенции, такие законодательные и иные меры, какие могут потребоваться для того, чтобы:

a) гарантировать такое оперативное обеспечение сохранности данных о трафике независимо от того, сколько поставщиков услуг было вовлечено в передачу того или иного сообщения; и

b) гарантировать оперативное раскрытие компетентному органу этого Государства-участника или лицу, назначенному этим компетентным органом, достаточного количества данных о трафике, которое позволит Государству-участнику идентифицировать поставщиков услуг и путь, по которому передавалось сообщение или указанная информация.

Статья 27. Распоряжение о предоставлении информации

Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться для наделения его компетентных органов полномочиями давать распоряжения:

a) лицу на своей территории предоставить конкретные электронные данные, находящиеся во владении или под контролем этого лица, которые хранятся в информационно-коммуникационной системе или на носителе электронных данных; и

b) поставщику услуг, предлагающему свои услуги на территории Государства-участника, предоставить абонентские данные, имеющие отношение к этим услугам и находящиеся во владении или под контролем этого поставщика услуг.

Статья 28. Обыск и изъятие хранимых электронных данных

1. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться для предоставления его компетентным органам полномочий проводить обыск или аналогичные мероприятия для получения доступа:

a) к информационно-коммуникационной системе, ее части и хранящимся в них электронным данным и

b) к носителю электронных данных, на котором могут храниться искомые электронные данные;

на территории этого Государства-участника.

2. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться, с тем чтобы в тех случаях, когда его органы проводят обыск или аналогичные мероприятия для получения доступа к конкретной информационно-коммуникационной системе или ее части в соответствии с подпунктом (a) пункта 1 настоящей статьи и имеют основания полагать, что искомые электронные данные хранятся в другой информационно-коммуникационной системе или ее части на его территории, и доступ к таким данным может быть законно получен из первоначальной системы или они находятся в ее распоряжении, эти органы могли оперативно провести обыск для получения доступа к этой другой информационно-коммуникационной системе.

3. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться для предоставления его компетентным органам полномочий производить изъятие или аналогичным образом обеспечивать сохранность электронных данных на своей территории, доступ к которым получен в соответствии с пунктом 1 или 2 настоящей статьи. Эти меры включают предоставление следующих полномочий:

a) производить изъятие или аналогичным образом обеспечивать сохранность информационно-коммуникационной системы или ее части или носителя электронных данных;

b) изготавливать и сохранять копии таких электронных данных в электронной форме;

c) обеспечивать целостность соответствующих хранимых электронных данных;

d) делать недоступными или удалять эти электронные данные в информационно-коммуникационной системе, к которой был получен доступ.

4. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться для предоставления его компетентным органам полномочий привлекать любое лицо, обладающее знаниями о функционировании соответствующей информационно-коммуникационной системы, информационно-телекоммуникационной сети или их составных частей или мерах, применяемых для защиты содержащихся в ней электронных данных, с целью предоставления в разумных пределах необходимых сведений для содействия осуществлению мер, указанных в пунктах 1—3 настоящей статьи.

Статья 29. Сбор в режиме реального времени данных о трафике

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

a) собирать или записывать с применением технических средств на территории этого Государства-участника и

i) собирать или записывать с применением технических средств на территории этого Государства-участника или

ii) сотрудничать с компетентными органами и помогать им собирать или записывать;

в режиме реального времени данные о трафике, относящиеся к конкретным сообщениям на его территории, передаваемым с помощью информационно-коммуникационной системы.

2. Если какое-либо Государство-участник в силу принципов своей внутренней правовой системы не может принять меры, указанные в подпункте (a) пункта 1 настоящей статьи, то вместо этого оно может принять такие законодательные и иные меры, какие могут потребоваться для обеспечения сбора или записи в режиме реального времени данных о трафике, относящихся к конкретным сообщениям, передаваемым на его территории, с применением технических средств на этой территории.

3. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться, с тем чтобы обязать постав-

щика услуг соблюдать конфиденциальность факта осуществления любых полномочий, предусмотренных в настоящей статье, и любой информации об этом.

Статья 30. Перехват данных о содержании

1. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться в связи с рядом серьезных уголовных правонарушений, подлежащих определению в его внутреннем законодательстве, для предоставления его компетентным органам полномочий:

a) собирать или записывать с применением технических средств на территории этого Государства-участника и

i) собирать или записывать с применением технических средств на территории этого Государства-участника; или

ii) сотрудничать с компетентными органами и помогать им собирать или записывать;

в режиме реального времени данные о содержании конкретных сообщений, передаваемых на его территории с помощью информационно-коммуникационной системы.

2. Если какое-либо Государство-участник в силу принципов своей внутренней правовой системы не может принять меры, указанные в подпункте (a) пункта 1 настоящей статьи, то вместо этого оно может принять законодательные и иные меры, какие могут потребоваться для обеспечения сбора или записи в режиме реального времени данных о содержании конкретных сообщений на его территории с применением технических средств на этой территории.

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

Статья 31. Замораживание, арест и конфискация доходов от преступлений

1. Каждое Государство-участник принимает в максимальной степени, возможной в рамках своей внутренней правовой системы, такие меры, какие могут потребоваться для обеспечения возможности конфискации:

a) доходов от преступлений, признанных таковыми в соответствии с настоящей Конвенцией, или имущества, стоимость которого соответствует таким доходам;

b) имущества, оборудования и других средств, использовавшихся или предназначавшихся для использования при совершении преступлений, признанных таковыми в соответствии с настоящей Конвенцией.

2. Каждое Государство-участник принимает такие меры, какие могут потребоваться для обеспечения возможности выявления, отслеживания, замораживания или ареста любого из перечисленного в пункте 1 настоящей статьи с целью последующей конфискации.

3. Каждое Государство-участник принимает в соответствии со своим внутренним законодательством такие законодательные и иные меры, какие могут потребоваться для регулирования управления компетентными органами замороженным, арестованным или конфискованным имуществом, указанным в пунктах 1 и 2 настоящей статьи.

4. Если доходы от преступлений были превращены или преобразованы, частично или полностью, в другое имущество, то меры, указанные в настоящей статье, применяются в отношении такого имущества, а не доходов.

5. Если доходы от преступлений были приобщены к имуществу, приобретенному из законных источников, то конфискации, без ущерба для любых полномочий, касающихся замораживания или ареста, подлежит та часть имущества, которая соответствует оцененной стоимости приобщенных доходов от преступлений.

6. К прибыли или другим выгодам, которые получены от доходов от преступлений, от имущества, в которое были превращены или преобразованы доходы от преступлений, или от имущества, к которому были приобщены доходы от преступлений, также применяются меры, указанные в настоящей статье, таким же образом и в той же степени, как и в отношении доходов от преступлений.

7. Для целей настоящей статьи и статьи 50 настоящей Конвенции каждое Государство-участник уполномочивает свои суды или другие компетентные органы издавать постановления о представлении или изъятии банковских, финансовых или коммерческих документов. Государство-участник не отказывается от принятия мер в соответствии с положениями настоящего пункта, ссылаясь на необходимость сохранения банковской тайны.

8. Каждое Государство-участник может рассмотреть возможность установления требования о том, чтобы лицо, совершившее преступление, доказало законное происхождение предполагаемых доходов от

преступления или другого имущества, подлежащего конфискации, в той мере, в какой такое требование соответствует принципам его внутреннего законодательства и характеру судебного и иного разбирательства.

9. Положения настоящей статьи не толкуются таким образом, чтобы наносился ущерб правам добросовестных третьих сторон.

10. Ничто содержащееся в настоящей статье не затрагивает принципа, согласно которому меры, о которых в ней говорится, определяются и осуществляются в соответствии с положениями внутреннего законодательства Государства-участника.

Статья 32. Сведения о судимости

Каждое Государство-участник может принимать такие законодательные или иные меры, какие могут потребоваться для учета, на таких условиях и в таких целях, какие оно сочтет надлежащими, любого ранее вынесенного в другом государстве обвинительного приговора в отношении лица, предположительно совершившего преступление, для использования такой информации в ходе уголовного производства в связи с преступлением, признанным таковым в соответствии с настоящей Конвенцией.

Статья 33. Защита свидетелей

1. Каждое Государство-участник принимает в соответствии со своим внутренним законодательством и в пределах своих возможностей надлежащие меры для обеспечения эффективной защиты от вероятной мести или запугивания в отношении свидетелей, которые дают показания или добросовестно и на разумных основаниях предоставляют информацию о преступлениях, признанных таковыми в соответствии с настоящей Конвенцией, или иным образом сотрудничают со следственными или судебными органами, и, в надлежащих случаях, в отношении их родственников и других близких им лиц.

2. Меры, предусмотренные в пункте 1 настоящей статьи, без ущерба для прав обвиняемого, в том числе для права на надлежащее разбирательство, могут, среди прочего, включать:

a) установление процедур для физической защиты таких лиц, например, в той мере, в какой это необходимо и практически осуществимо, для их переселения в другое место, и принятие таких положений, какие разрешают, в надлежащих случаях, не разглашать информацию, касающуюся личности и местонахождения таких лиц, или устанавливают ограничения на разглашение такой информации;

b) принятие правил доказывания, обеспечивающих безопасность свидетелей при даче показаний, например правил, разрешающих давать показания с помощью коммуникационных технологий, таких как видеосвязь, или других надлежащих средств.

3. Государства-участники рассматривают вопрос о заключении с другими государствами соглашений или договоренностей относительно переселения лиц, указанных в пункте 1 настоящей статьи.

4. Положения настоящей статьи применяются также в отношении потерпевших в той мере, в какой они являются свидетелями.

Статья 34. Помощь потерпевшим и их защита

1. Каждое Государство-участник принимает в пределах своих возможностей надлежащие меры для предоставления помощи и защиты потерпевшим от преступлений, признанных таковыми в соответствии с настоящей Конвенцией, особенно в случаях угрозы местью или запугивания.

2. Каждое Государство-участник при условии соблюдения своего внутреннего законодательства устанавливает надлежащие процедуры для обеспечения доступа к компенсации и возмещению ущерба потерпевшим от преступлений, признанных таковыми в соответствии с настоящей Конвенцией.

3. Каждое Государство-участник при условии соблюдения своего внутреннего законодательства создает возможности для изложения и рассмотрения мнений и опасений потерпевших на соответствующих стадиях уголовного производства в отношении лиц, совершивших преступления, таким образом, чтобы это не наносило ущерба правам защиты.

4. В отношении преступлений, признанных таковыми в соответствии со статьями 14—16 настоящей Конвенции, каждое Государство-участник при условии соблюдения своего внутреннего законодательства принимает меры с целью оказания помощи потерпевшим от таких преступлений, в том числе для обеспечения их физического и психологического восстановления, в сотрудничестве с соответствующими международными организациями, неправительственными организациями и другими субъектами гражданского общества.

5. При применении положений пунктов 2—4 настоящей статьи каждое Государство-участник принимает во внимание возраст, пол и

особые обстоятельства и потребности потерпевших, включая особые обстоятельства и потребности детей.

6. Каждое Государство-участник в той мере, в какой это соответствует требованиям его национальной нормативно-правовой базы, принимает эффективные меры для обеспечения выполнения просьб об удалении или обеспечении недоступности материалов, указанных в статьях 14 и 16 настоящей Конвенции.

Глава V. Международное сотрудничество

Статья 35. Общие принципы международного сотрудничества

1. Государства-участники сотрудничают друг с другом в соответствии с положениями настоящей Конвенции и других применимых международных документов о международном сотрудничестве в уголовно-правовых вопросах и нормами внутреннего законодательства в целях:

a) осуществления расследования, уголовного преследования и судебного разбирательства в отношении уголовных правонарушений, признанных таковыми в соответствии с настоящей Конвенцией, в том числе в целях замораживания, ареста, конфискации и возвращения доходов от таких правонарушений;

b) сбора, получения, обеспечения сохранности и передачи доказательств в электронной форме по уголовным правонарушениям, признанным таковыми в соответствии с настоящей Конвенцией;

c) сбора, получения, обеспечения сохранности и передачи доказательств в электронной форме по любому серьезному преступлению, включая серьезные преступления, признанные таковыми в соответствии с другими применимыми конвенциями и протоколами Организации Объединенных Наций, действовавшими на момент принятия настоящей Конвенции.

2. Для целей сбора, получения, обеспечения сохранности и передачи доказательств в электронной форме по преступлениям, предусмотренным в подпунктах (b) и (c) пункта 1 настоящей статьи, применяются соответствующие пункты статьи 40 и статей 41—46 настоящей Конвенции.

3. 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 описывает ли оно 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.

Статья 36. Защита персональных данных

1. a) Государство-участник, передающее персональные данные в соответствии с настоящей Конвенцией, делает это в соответствии со своим внутренним законодательством и любыми возможными обязательствами передающей стороны по применимым нормам международного права. Государства-участники не обязаны передавать персональные данные в соответствии с настоящей Конвенцией, если эти данные не могут быть предоставлены в соответствии с их применимыми законами, касающимися защиты персональных данных.

b) Если передача персональных данных противоречит подпункту (a) пункта 1 настоящей статьи, государства-участники могут принимать меры к установлению в соответствии с такими применимыми законами надлежащих условий для обеспечения выполнения требований, необходимых для удовлетворения просьбы о предоставлении персональных данных.

c) Государствам-участникам рекомендуется заключать двусторонние или многосторонние договоренности для облегчения передачи персональных данных.

2. При передаче персональных данных в соответствии с настоящей Конвенцией государства-участники обеспечивают, чтобы на полученные персональные данные распространялись эффективные и надлежащие гарантии, предусмотренные соответствующей нормативно-правовой базой государств-участников.

3. Для передачи персональных данных, полученных в соответствии с настоящей Конвенцией, третьей стране или международной организации Государство-участник уведомляет первое передающее Государство-участник о своем намерении и запрашивает у него разрешение. Государство-участник передает персональные данные только с разрешения первого передающего Государства-участника, которое может потребовать, чтобы разрешение предоставлялось в письменной форме.

Статья 37. Выдача

1. Настоящая статья применяется к уголовным правонарушениям, признанным таковыми в соответствии с настоящей Конвенцией, если лицо, в отношении которого направлен запрос о выдаче, находится на территории запрашиваемого Государства-участника, при условии, что правонарушение, в связи с которым запрашивается выдача, является уголовно наказуемым по внутреннему законодательству как запрашивающего Государства-участника, так и запрашиваемого Государства-участника. Когда выдача запрашивается для целей отбывания осужденным окончательного наказания в виде тюремного заключения или другой формы содержания под стражей, назначенного за правонарушение, влекущее выдачу, запрашиваемое Государство-участник может удовлетворить просьбу о выдаче в соответствии с внутренним законодательством.

2. Невзирая на положения пункта 1 настоящей статьи, Государство-участник, законодательство которого допускает это, может разрешить выдачу какого-либо лица в связи с любым из уголовных правонарушений, признанных таковыми в соответствии с настоящей Конвенцией, которые не являются уголовно наказуемыми согласно его собственному внутреннему законодательству.

3. Если просьба о выдаче касается нескольких отдельных уголовных правонарушений, по меньшей мере одно из которых может повлечь за собой выдачу согласно настоящей статье, а другие не могут повлечь выдачу по причине срока лишения свободы 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. Каждое из преступлений, к которым применяется настоящая статья, считается включенным в любой существующий между государствами-участниками договор о выдаче в качестве преступления, которое может 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.

5. Если Государство-участник, обусловливающее выдачу наличием договора, получает просьбу о выдаче от другого Государства-участника, с которым у него не заключен договор о выдаче, оно может рассматривать настоящую Конвенцию в качестве правового основания для выдачи в связи с любым преступлением, к которому применяется настоящая статья.

6. Государства-участники, обусловливающие выдачу наличием договора:

a) при сдаче на хранение своих ратификационных грамот или документов о принятии или утверждении настоящей Конвенции или присоединении к ней сообщают Генеральному секретарю Организации Объединенных Наций о том, будут ли они использовать настоящую Конвенцию в качестве правового основания для сотрудничества в вопросах выдачи с другими государствами — участниками настоящей Конвенции; и

b) если они не используют настоящую Конвенцию в качестве правового основания для сотрудничества в вопросах выдачи, стремятся, в надлежащих случаях, к заключению договоров о выдаче с другими государствами — участниками настоящей Конвенции в целях применения настоящей статьи.

7. 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.

8. 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.

9. В отношении любого преступления, к которому применяется настоящая статья, государства-участники при условии соблюдения своего внутреннего законодательства прилагают усилия к тому, чтобы ускорить процедуры выдачи и упростить связанные с ней требования о предоставлении доказательств.

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, в том числе когда просьба направляется по существующим каналам Международной организации уголовной полиции, 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.

11. Государство-участник, на территории которого находится лицо, предположительно совершившее преступление, если оно не выдает

такое лицо в связи с преступлением, к которому применяется настоящая статья, лишь на том основании, что оно является одним из его граждан, обязано, по просьбе Государства-участника, запрашивающего выдачу, передать дело без неоправданных задержек своим компетентным органам для цели уголовного преследования. Эти органы принимают свои решения и осуществляют производство таким же образом, как и в случае любого другого преступления сопоставимого характера согласно внутреннему законодательству этого Государства-участника. Заинтересованные государства-участники сотрудничают друг с другом, в частности в процессуальных вопросах и вопросах доказывания, для обеспечения эффективности такого уголовного 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 11 настоящей статьи.

13. Если в выдаче, которая запрашивается в целях приведения приговора в исполнение, отказано, поскольку разыскиваемое лицо является гражданином запрашиваемого Государства-участника, запрашиваемое Государство-участник, если это допускает его внутреннее законодательство и в соответствии с требованиями такого законодательства, по обращению запрашивающего Государства-участника рассматривает вопрос о приведении в исполнение приговора или оставшейся части приговора, вынесенного согласно внутреннему законодательству запрашивающего Государства-участника.

14. 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 внутренним законодательством Государства-участника, на территории которого находится это лицо.

15. Ничто в настоящей Конвенции не толкуется как установление обязательства о выдаче, если у запрашиваемого Государства-участника имеются существенные основания полагать, что просьба о выдаче имеет целью уголовное преследование или наказание какого-либо лица по причине его пола, расы, языка, вероисповедания, гражданства, этнического происхождения или политических убеждений или что удовлетворение этой просьбы нанесло бы ущерб положению этого лица по любой из этих причин.

16. Государства-участники не могут отказывать в выполнении просьбы о выдаче лишь на том основании, что преступление считается также связанным с налоговыми вопросами.

17. 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 предоставления информации, имеющей отношение к изложенным в его просьбе утверждениям.

18. Запрашиваемое Государство-участник информирует запрашивающее Государство-участник о своем решении относительно выдачи. Запрашиваемое государство-участник информирует запрашивающее Государство-участник о любых причинах отказа в выдаче, за исключением случаев, когда запрашиваемое Государство-участник не может этого сделать в силу своего внутреннего законодательства или своих международно-правовых обязательств.

19. Каждое Государство-участник в момент подписания или при сдаче на хранение своего документа о ратификации, принятии, утверждении или присоединении сообщает Генеральному секретарю Организации Объединенных Наций название и адрес органа, ответственного за направление или получение просьб о выдаче или предварительном задержании. Генеральный секретарь составляет и обновляет реестр органов, назначенных государствами-участниками для указанных целей. Каждое Государство-участник постоянно обеспечивает достоверность сведений, содержащихся в реестре.

20. Государства-участники стремятся заключать двусторонние и многосторонние соглашения или договоренности с целью осуществления или повышения эффективности выдачи.

Статья 38. Передача осужденных лиц

Государства-участники могут, принимая во внимание права осужденных лиц, рассматривать возможность заключения двусторонних или многосторонних соглашений или договоренностей о передаче лиц, осужденных к тюремному заключению или другим видам лишения сво-

боды за преступления, признанные таковыми в соответствии с настоящей Конвенцией, с тем чтобы они могли отбывать срок наказания на их территории. Государства-участники могут также принимать во внимание вопросы, касающиеся согласия, реабилитации и реинтеграции.

Статья 39. Передача уголовного производства

1. Государства-участники рассматривают возможность взаимной передачи производства в целях уголовного преследования в связи с преступлением, признанным таковым в соответствии с настоящей Конвенцией, когда считается, что такая передача отвечает интересам надлежащего отправления правосудия, в частности в случаях, когда затрагиваются несколько юрисдикций, для обеспечения объединения уголовных дел.

2. Если Государство-участник, обусловливающее передачу уголовного производства наличием договора, получает просьбу о передаче от другого Государства-участника, с которым у него не заключен договор по данному вопросу, оно может рассматривать настоящую Конвенцию в качестве правового основания для передачи уголовного производства в связи с любым преступлением, к которому применима настоящая статья.

Статья 40. Общие принципы и процедуры взаимной правовой помощи

1. Государства-участники оказывают друг другу самую широкую взаимную правовую помощь в расследовании, уголовном преследовании и судебном разбирательстве в связи с преступлениями, признанными таковыми в соответствии с настоящей Конвенцией, а также в сборе доказательств в электронной форме о преступлениях, признанных таковыми в соответствии с настоящей Конвенцией, а также о серьезных преступлениях.

2. Взаимная правовая помощь предоставляется в объеме, максимально возможном согласно соответствующим законам, международным договорам, соглашениям и договоренностям запрашиваемого Государства-участника в отношении расследования, уголовного преследования и судебного разбирательства в связи с преступлениями, за совершение которых к ответственности в запрашивающем Государстве-участнике может быть привлечено юридическое лицо в соответствии со статьей 18 настоящей Конвенции.

3. Взаимная правовая помощь, предоставляемая в соответствии с настоящей статьей, может запрашиваться с любой из следующих целей:

a) получение показаний или заявлений от лиц;

b) вручение судебных документов;

c) проведение обыска, изъятия и замораживания;

d) проведение обыска или аналогичных мероприятий для получения доступа к электронным данным, хранимым в информационно-коммуникационной системе, их изъятие или аналогичные действия для обеспечения их сохранности и их раскрытие в соответствии со статьей 44 настоящей Конвенции;

e) сбор в режиме реального времени данных о трафике в соответствии со статьей 45 настоящей Конвенции;

f) перехват данных о содержании в соответствии со статьей 46 настоящей Конвенции;

g) осмотр объектов и участков местности;

h) предоставление информации, доказательств и заключений экспертов;

i) предоставление подлинников или заверенных копий соответствующих документов и материалов, включая правительственные, банковские, финансовые, корпоративные или коммерческие документы;

j) выявление или отслеживание доходов от преступлений, имущества, средств совершения преступлений или других предметов для целей доказывания;

k) содействие добровольной явке соответствующих лиц в органы запрашивающего Государства-участника;

l) возвращение доходов от преступлений;

m) оказание любого иного вида помощи, не противоречащего внутреннему законодательству запрашиваемого Государства-участника.

4. Без ущерба для внутреннего законодательства компетентные органы Государства-участника могут без предварительной просьбы передавать информацию, касающуюся уголовно-правовых вопросов, компетентному органу в другом Государстве-участнике в тех случаях, когда они считают, что такая информация может помочь этому органу в осуществлении или успешном завершении расследования и уголовного разбирательства или может привести к просьбе, составленной этим Государством-участником в соответствии с настоящей Конвенцией.

5. Передача информации согласно пункту 4 настоящей статьи осуществляется без ущерба расследованию и уголовному производству в государстве компетентных органов, предоставляющих информацию.

Компетентные органы, получающие информацию, выполняют просьбу о сохранении конфиденциального характера этой информации, даже на временной основе, или соблюдают ограничения на ее использование. Это, однако, не препятствует тому, чтобы Государство-участник, получающее информацию, раскрывало в ходе проводимого в нем производства ту информацию, которая оправдывает обвиняемого. В таком случае до раскрытия информации Государство-участник, получающее информацию, уведомляет Государство-участник, предоставляющее информацию, и, если получена просьба об этом, проводит консультации с Государством-участником, предоставляющим информацию. Если, в исключительных случаях, заблаговременное уведомление невозможно, то

Государство-участник, получающее информацию, незамедлительно сообщает о таком раскрытии Государству-участнику, предоставляющему информацию.

6. Положения настоящей статьи не затрагивают обязательств по какому-либо другому договору, будь то двустороннему или многостороннему, который регулирует или будет регулировать, полностью или частично, взаимную правовую помощь.

7. Пункты 8—31 настоящей статьи применяются к просьбам, направленным на основании настоящей статьи, если соответствующие государства-участники не связаны каким-либо договором о взаимной правовой помощи. Если эти государства-участники связаны таким договором, то применяются соответствующие положения этого договора, если только государства-участники не соглашаются применять вместо них пункты 8—31 настоящей статьи. Государствам-участникам настоятельно рекомендуется применять положения этих пунктов, если это способствует сотрудничеству.

8. Государства-участники могут отказать в предоставлении помощи согласно настоящей статье на основании отсутствия обоюдного признания соответствующего деяния преступлением. Однако запрашиваемое Государство-участник может, если оно сочтет это надлежащим, предоставить помощь, объем которой оно определяет по своему усмотрению, независимо от того, является ли соответствующее деяние преступлением согласно внутреннему законодательству запрашиваемого Государства-участника. В помощи может быть отказано, когда просьбы касаются малозначительных вопросов или вопросов, в связи с которыми запрашиваемые сотрудничество или помощь могут быть обеспечены согласно другим положениям настоящей Конвенции.

9. Лицо, которое находится под стражей или отбывает наказание на территории одного Государства-участника и присутствие которого в другом Государстве-участнике требуется для целей установления личности, дачи показаний или оказания иной помощи в получении доказательств для расследования, уголовного преследования или судебного разбирательства в связи с преступлениями, признанными таковыми в соответствии с настоящей Конвенцией, может быть передано при соблюдении следующих условий:

a) данное лицо свободно дает на это свое осознанное согласие;

b) компетентные органы обоих государств-участников достигли согласия на таких условиях, которые эти государства-участники могут счесть надлежащими.

10. Для целей пункта 9 настоящей статьи:

a) Государство-участник, которому передается лицо, вправе и обязано содержать переданное лицо под стражей, если только Государство-участник, которое передало это лицо, не просило об ином или не санкционировало иное;

b) Государство-участник, которому передается лицо, незамедлительно выполняет свое обязательство по возвращению этого лица в распоряжение Государства-участника, которое передало это лицо, как это было согласовано заранее или как это было иным образом согласовано компетентными органами обоих государств-участников;

c) Государство-участник, которому передается лицо, не требует от Государства-участника, которое передало это лицо, возбуждения процедуры выдачи для его возвращения;

d) переданному лицу в срок наказания, отбываемого в государстве, которое его передало, засчитывается срок содержания под стражей в Государстве-участнике, которому оно передано.

11. Без согласия Государства-участника, которое в соответствии с пунктами 9 и 10 настоящей статьи должно передать какое-либо лицо, это лицо, независимо от его гражданства, не подвергается уголовному преследованию, заключению под стражу, наказанию или какому-либо другому ограничению свободы на территории государства, которому передается это лицо, в связи с действием, бездействием или осуждением, относящимися к периоду до его отбытия с территории государства, которое передало это лицо.

12. a) Каждое Государство-участник назначает центральный орган или органы, которые несут ответственность за получение просьб об оказании взаимной правовой помощи и либо за их выполнение, либо за их препровождение для выполнения компетентным органам и об-

ладают соответствующими полномочиями. Если в Государстве-участнике имеется специальный регион или территория с отдельной системой оказания взаимной правовой помощи, оно может назначить особый центральный орган, который будет выполнять такую же функцию в отношении этого региона или территории.

b) Центральные органы обеспечивают оперативное и надлежащее выполнение или препровождение полученных просьб. Если центральный орган препровождает просьбу для выполнения компетентному органу, он содействует оперативному и надлежащему выполнению этой просьбы компетентным органом.

c) При сдаче на хранение каждым 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, и составляет и обновляет реестр центральных органов, назначенных государствами-участниками. Каждое Государство-участник постоянно обеспечивает достоверность сведений, содержащихся в реестре.

d) Просьбы об оказании взаимной правовой помощи и любые относящиеся к ним сообщения препровождаются центральным органам, назначенным государствами-участниками. Это требование не наносит ущерба праву Государства-участника потребовать, чтобы такие просьбы и сообщения направлялись ему по дипломатическим каналам и, в случае чрезвычайных обстоятельств, когда государства-участники договорились об этом, через Международную организацию уголовной полиции, если это возможно.

13. Просьбы направляются в письменной форме или, если это возможно, с помощью любых средств, предоставляющих возможность составить письменную запись, на языке, приемлемом для запрашиваемого Государства-участника, при условиях, позволяющих этому Государству-участнику установить подлинность. При сдаче на хранение ратификационной грамоты или документа о принятии или утверждении настоящей Конвенции или присоединении к ней Генеральный секретарь Организации Объединенных Наций уведомляется о языке или языках, приемлемых для каждого Государства-участника. При чрезвычайных обстоятельствах и в случае согласования этого Государствами-участниками просьбы могут направляться в устной форме, однако они незамедлительно подтверждаются в письменной форме.

14. Если это не запрещено соответствующими законами государств-участников, их центральным органам рекомендуется передавать и получать просьбы о взаимной правовой помощи и связанные с ними сообщения, а также доказательства в электронной форме при условиях, позволяющих запрашиваемому Государству-участнику установить подлинность и обеспечивающих защищенность сообщений.

15. В просьбе об оказании взаимной правовой помощи указываются:

a) наименование органа, обращающегося с просьбой;

b) существо вопроса и характер расследования, уголовного преследования или судебного разбирательства, к которым относится просьба, а также наименование и функции органа, осуществляющего это расследование, уголовное преследование или судебное разбирательство;

c) краткое изложение соответствующих фактов, за исключением того, что касается просьб в отношении вручения судебных документов;

d) описание запрашиваемой помощи и подробная информация о любой конкретной процедуре, соблюдение которой хотело бы обеспечить запрашивающее Государство-участник;

e) если это возможно и уместно, данные о личности, местонахождении и гражданстве любого соответствующего лица, а также название страны происхождения, описание и местонахождение соответствующего предмета или счетов;

f) в соответствующих случаях — промежуток времени, за который запрашиваются доказательства, информация или другая помощь;

g) цель, для которой запрашиваются доказательства, информация или другая помощь.

16. Запрашиваемое Государство-участник может запросить дополнительную информацию, если эта информация представляется необходимой для выполнения просьбы в соответствии с его внутренним законодательством или если эта информация может облегчить выполнение такой просьбы.

17. Просьба выполняется в соответствии с внутренним законодательством запрашиваемого Государства-участника и в той мере, в какой это не противоречит внутреннему законодательству запрашиваемого Государства-участника, по возможности, в соответствии с указанными в просьбе процедурами.

18. В той мере, в какой это возможно и соответствует основополагающим принципам внутреннего законодательства, если какое-либо лицо находится на территории Государства-участника и должно быть допрошено в качестве свидетеля, потерпевшего или эксперта судебными органами другого Государства-участника, первое Государство-

участник может, по просьбе другого Государства-участника, разрешить проведение допроса с помощью видео-конференц-связи, если личное присутствие соответствующего лица на территории запрашивающего Государства-участника не является возможным или желательным. Государства-участники могут договориться о том, что допрос проводится судебным органом запрашивающего Государства-участника в присутствии судебного органа запрашиваемого Государства-участника. Если запрашиваемое Государство-участник не имеет доступа к техническим средствам для проведения сеанса видеоконференц-связи, такие средства по взаимной договоренности могут быть предоставлены ему запрашивающим Государством-участником.

19. Запрашивающее Государство-участник не передает и не использует информацию или доказательства, представленные запрашиваемым Государством-участником, для осуществления расследования, уголовного преследования или судебного разбирательства, иного, чем то, которое указано в просьбе, без предварительного согласия на это запрашиваемого Государства-участника. Ничто в настоящем пункте не препятствует запрашивающему Государству-участнику раскрывать в ходе проводимого в нем производства ту информацию или доказательства, которые оправдывают обвиняемого. В этом случае до раскрытия информации или доказательств запрашивающее Государство-участник уведомляет запрашиваемое Государство-участник и, если получена просьба об этом, проводит консультации с запрашиваемым Государством-участником. Если, в исключительных случаях, заблаговременное уведомление невозможно, то запрашивающее Государство-участник незамедлительно сообщает о таком раскрытии запрашиваемому Государству-участнику.

20. Запрашивающее Государство-участник может потребовать, чтобы запрашиваемое Государство-участник сохраняло конфиденциальность наличия и существа просьбы, за исключением того, что необходимо для выполнения самой просьбы. Если запрашиваемое Государство-участник не может выполнить требование о конфиденциальности, оно незамедлительно сообщает об этом запрашивающему Государству-участнику.

21. Во взаимной правовой помощи может быть отказано:

a) если просьба не была представлена в соответствии с положениями настоящей статьи;

b) если запрашиваемое Государство-участник считает, что выполнение просьбы может нанести ущерб его суверенитету, безопасности, публичному порядку или другим жизненно важным интересам;

c) если внутреннее законодательство запрашиваемого Государства-участника запрещает его органам осуществлять запрашиваемые меры в отношении любого аналогичного преступления, если бы такое преступление являлось предметом расследования, преследования или судебного разбирательства в пределах его юрисдикции;

d) если выполнение просьбы противоречит требованиям правовой системы запрашиваемого Государства-участника в части, касающейся взаимной правовой помощи.

22. Ничто в настоящей Конвенции не толкуется как установление обязательства оказывать взаимную правовую помощь, если у запрашиваемого Государства-участника имеются веские основания полагать, что просьба о помощи имеет целью преследование или наказание какого-либо лица по причине его пола, расы, языка, вероисповедания, гражданства, этнического происхождения или политических убеждений или что удовлетворение этой просьбы нанесло бы ущерб положению этого лица по любой из этих причин.

23. Государства-участники не могут отказывать в выполнении просьбы о взаимной правовой помощи лишь на том основании, что преступление считается также связанным с налоговыми вопросами.

24. Государства-участники не отказывают в предоставлении взаимной правовой помощи согласно настоящей статье на основании банковской тайны.

25. Любой отказ в предоставлении взаимной правовой помощи мотивируется.

26. Запрашиваемое Государство-участник выполняет просьбу об оказании взаимной правовой помощи в возможно короткие сроки и, насколько это возможно, полностью учитывает любые предельные сроки, которые предложены запрашивающим Государством-участником и которые мотивированы, предпочтительно в самой просьбе. Запрашиваемое Государство-участник отвечает на разумные запросы запрашивающего Государства-участника относительно статуса и хода выполнения просьбы. Запрашивающее Государство-участник оперативно сообщает запрашиваемому Государству-участнику о том, что необходимости в запрошенной помощи более не имеется.

27. Оказание взаимной правовой помощи может быть отсрочено запрашиваемым Государством-участником на том основании, что это воспрепятствует осуществляемому расследованию, преследованию или судебному разбирательству.

28. До отказа в выполнении просьбы согласно пункту 21 настоящей статьи или отсрочки ее выполнения согласно пункту 27 настоящей

статьи запрашиваемое Государство-участник проводит консультации с запрашивающим Государством-участником, для того чтобы определить, может ли помощь быть предоставлена в такие сроки и на таких условиях, какие запрашиваемое Государство-участник считает необходимыми. Если запрашивающее Государство-участник принимает помощь на таких условиях, то оно соблюдает данные условия.

29. Без ущерба для применения пункта 11 настоящей статьи свидетель, эксперт или иное лицо, которое, по просьбе запрашивающего Государства-участника, соглашается давать показания в ходе производства или оказывать помощь при осуществлении расследования, преследования или судебного разбирательства на территории запрашивающего Государства-участника, не подвергается уголовному преследованию, заключению под стражу, наказанию или какому-либо другому ограничению личной свободы на этой территории в связи с действием, бездействием или осуждением, относящимися к периоду до его отбытия с территории запрашиваемого Государства-участника. Действие такой гарантии личной безопасности прекращается, если свидетель, эксперт или иное лицо в течение 15 последовательных дней или в течение любого согласованного между государствами-участниками срока, начиная с даты, когда такое лицо было официально уведомлено о том, что его присутствие более не требуется судебным органам, имело возможность покинуть территорию запрашивающего Государства-участника, но тем не менее добровольно осталось на этой территории или, покинув ее, возвратилось назад по собственной воле.

30. Обычные расходы, связанные с выполнением просьбы, покрываются запрашиваемым Государством-участником, если заинтересованные государства-участники не договорились об ином. Если выполнение просьбы требует или потребует существенных или чрезвычайных расходов, то государства-участники проводят консультации с целью определения условий, на которых будет выполнена просьба, а также порядка покрытия расходов.

31. Запрашиваемое Государство-участник:

a) предоставляет запрашивающему Государству-участнику копии правительственных материалов, документов или информации, которыми оно располагает и которые согласно его внутреннему законодательству открыты для публичного доступа;

b) может по своему усмотрению предоставлять запрашивающему Государству-участнику полностью или частично или при соблюдении таких условий, какие оно считает надлежащими, копии любых правительственных материалов, документов или информации, которыми

оно располагает и которые согласно его внутреннему законодательству закрыты для публичного доступа.

32. Государства-участники рассматривают, по мере необходимости, возможность заключения двусторонних или многосторонних соглашений или договоренностей, которые отвечали бы целям настоящей статьи, обеспечивали бы ее действие на практике или укрепляли бы ее положения.

Статья 41. Сеть 24/7

1. Каждое Государство-участник назначает контактный центр, работающий 24 часа в сутки 7 дней в неделю, для обеспечения предоставления неотложной помощи в целях осуществления конкретных уголовных расследований, преследования или судебного разбирательства в связи с преступлениями, признанными таковыми в соответствии с настоящей Конвенцией, или для сбора, получения и обеспечения сохранности доказательств в электронной форме для целей пункта 3 настоящей статьи и в связи с преступлениями, признанными таковыми в соответствии с настоящей Конвенцией, и серьезными преступлениями.

2. Генеральный секретарь Организации Объединенных Наций уведомляется о таком контактном центре и ведет обновляемый реестр контактных центров, назначенных для целей настоящей статьи, и ежегодно распространяет среди государств-участников обновленный список контактных центров.

3. Такая помощь включает содействие применению или, если это допускается внутренним законодательством и практикой запрашиваемого Государства-участника, непосредственное применение следующих мер:

a) оказание технической консультационной помощи;

b) обеспечение сохранности хранимых электронных данных в соответствии со статьями 42 и 43 настоящей Конвенции, в том числе предоставление при необходимости информации о местонахождении поставщика услуг, если оно известно запрашиваемому Государству-участнику, для оказания содействия запрашивающему Государству-участнику в составлении запроса;

c) сбор доказательств и предоставление правовой информации;

d) определение местонахождения подозреваемых; или

e) предоставление электронных данных для предотвращения чрезвычайной ситуации.

4. Контактный центр Государства-участника должен располагать возможностями для оперативной связи с контактным центром другого Государства-участника. Если назначенный Государством-участником контактный центр не является структурным подразделением органа или органов этого Государства-участника, ответственных за оказание взаимной правовой помощи или выдачу, этот контактный центр обеспечивает возможность своего оперативного взаимодействия с таким органом или органами.

5. Каждое Государство-участник обеспечивает наличие подготовленного и оснащенного персонала для обеспечения функционирования сети 24/7.

6. Государства-участники могут также использовать и укреплять существующие уполномоченные сети контактных центров, где это применимо и в рамках их внутреннего законодательства, включая сети 24/7 Международной организации уголовной полиции по компьютерным преступлениям, для обеспечения быстрого взаимодействия между полицейскими органами и применения других методов сотрудничества в области обмена информацией.

Статья 42. Международное сотрудничество в целях оперативного обеспечения сохранности хранимых электронных данных

1. Государство-участник может обратиться к другому Государству-участнику с просьбой вынести соответствующее постановление или иным образом оперативно обеспечить в соответствии со статьей 25 настоящей Конвенции сохранность электронных данных, которые хранятся в информационно-коммуникационной системе на территории этого другого Государства-участника и в связи с которыми запрашивающее Государство-участник намерено направить просьбу об оказании взаимной правовой помощи в проведении обыска или аналогичных мероприятий для получения доступа к этим электронным данным, в осуществлении их изъятия или аналогичных действий для обеспечения их сохранности или в их раскрытии.

2. Запрашивающее Государство-участник может воспользоваться предусмотренной в статье 41 настоящей Конвенции сетью 24/7 для получения информации о местонахождении электронных данных, хранящихся с помощью информационно-коммуникационной системы, и при необходимости информации о местонахождении поставщика услуг.

3. В просьбе об обеспечении сохранности данных, направляемой в соответствии с пунктом 1 настоящей статьи, указываются:

a) орган, обращающийся с просьбой об обеспечении сохранности;

b) преступление, в связи с которым проводится уголовное расследование, преследование или судебное разбирательство, и краткое изложение относящихся к нему фактов;

c) хранимые электронные данные, сохранность которых требуется обеспечить, и их связь с преступлением;

d) любая имеющаяся информация, идентифицирующая хранителя хранимых электронных данных или местонахождение информационно-коммуникационной системы;

e) необходимость обеспечения сохранности данных;

f) сведения о намерении запрашивающего Государства-участника направить просьбу об оказании взаимной правовой помощи в проведении обыска или аналогичных мероприятий для получения доступа к хранимым электронным данным, осуществлении их изъятия или аналогичных действий для обеспечения их сохранности или в их раскрытии;

g) в соответствующих случаях — необходимость сохранять конфиденциальность просьбы об обеспечении сохранности и не уведомлять пользователя.

4. По получении просьбы от другого Государства-участника запрашиваемое Государство-участник принимает все надлежащие меры для оперативного обеспечения сохранности указанных в просьбе данных в соответствии со своим внутренним законодательством. Для целей удовлетворения просьбы обоюдное признание соответствующего деяния преступлением в качестве условия обеспечения такой сохранности не требуется.

5. Государство-участник, которое требует обоюдного признания соответствующего деяния преступлением в качестве условия для удовлетворения просьбы о взаимной правовой помощи в проведении обыска или аналогичных мероприятий для получения доступа к хранимым электронным данным, осуществлении их изъятия или аналогичных действий для обеспечения их сохранности или в их раскрытии, может в отношении преступлений, не признанных таковыми в соответствии с настоящей Конвенцией, оставить за собой право отказать в просьбе об обеспечении сохранности согласно настоящей статье в случаях, когда у него имеются основания полагать, что на момент раскрытия данных возможность выполнения условия об обоюдном признании соответствующего деяния преступлением будет отсутствовать.

6. Кроме того, в просьбе об обеспечении сохранности может быть отказано только на основаниях, указанных в подпунктах (b) и (c) пункта 21 и в пункте 22 статьи 40 настоящей Конвенции.

7. Если запрашиваемое Государство-участник считает, что обеспечение сохранности не обеспечит доступность данных в будущем или будет угрожать конфиденциальности или иным образом наносить ущерб проводимому запрашивающим Государством-участником расследованию, оно оперативно информирует об этом запрашивающее Государство-участник, которое в этом случае определяет, следует ли тем не менее выполнить данную просьбу.

8. Любые меры по обеспечению сохранности в ответ на просьбу, направленную в соответствии с пунктом 1 настоящей статьи, действуют в течение не менее 60 дней, с тем чтобы запрашивающее Государство-участник имело возможность направить просьбу о проведении обыска или аналогичных мероприятий для получения доступа к данным, осуществлении их изъятия или аналогичных действий для обеспечения их сохранности или об их раскрытии. После получения такой просьбы сохранность таких данных обеспечивается до принятия решения в отношении этой просьбы.

9. До истечения срока обеспечения сохранности, указанного в пункте 8 настоящей статьи, запрашивающее Государство-участник может запросить продление этого срока.

Статья 43. Международное сотрудничество в целях оперативного предоставления сохраненных данных о трафике

1. Если в ходе выполнения направленной в соответствии со статьей 42 настоящей Конвенции просьбы об обеспечении сохранности данных о трафике, относящихся к конкретному сообщению, запрашиваемому Государству-участнику станет известно, что в передаче сообщения участвовал поставщик услуг в другом Государстве-участнике, запрашиваемое Государство-участник оперативно раскрывает запрашивающему Государству-участнику данные о трафике в объеме, достаточном для идентификации этого поставщика услуг и определения маршрута передачи этого сообщения.

2. В просьбе о раскрытии данных о трафике в соответствии с пунктом 1 настоящей статьи может быть отказано только на основаниях, указанных в подпунктах (b) и (c) пункта 21 и в пункте 22 статьи 40 настоящей Конвенции.

Статья 44. Взаимная правовая помощь в получении доступа к хранимым электронным данным

1. Государство-участник может обратиться к другому Государству-участнику с просьбой о проведении обыска или аналогичных мероприятий для получения доступа к электронным данным, осуществлении изъятия или аналогичных действий для обеспечения сохранности или о раскрытии данных, хранящихся в информационно-коммуникационной системе на территории запрашиваемого Государства-участника, включая электронные данные, сохранность которых была обеспечена в соответствии со статьей 42 настоящей Конвенции.

2. Запрашиваемое Государство-участник отвечает на эту просьбу, следуя соответствующим международным документам и законам, указанным в статье 35 настоящей Конвенции, и согласно другим соответствующим положениям настоящей главы.

3. Ответ на просьбу дается в ускоренном порядке, если:

a) имеются основания полагать, что соответствующие данные особенно подвержены утрате или видоизменению; или

b) документы и законы, указанные в пункте 2 настоящей статьи, предусматривают иное сотрудничество в ускоренном порядке.

Статья 45. Взаимная правовая помощь в сборе в режиме реального времени данных о трафике

1. Государства-участники стремятся оказывать друг другу взаимную правовую помощь в сборе в режиме реального времени данных о трафике, относящихся к конкретным сообщениям, передаваемым на их территории с помощью информационно-коммуникационной системы. С учетом положений пункта 2 настоящей статьи такая помощь оказывается в соответствии с условиями и процедурами, предусмотренными внутренним законодательством.

2. Каждое Государство-участник стремится оказывать такую помощь по крайней мере в отношении уголовных правонарушений, в связи с которыми сбор данных о трафике в режиме реального времени был бы возможен в рамках аналогичного внутреннего дела.

3. В просьбе, направляемой 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 просьба;

c) электронные данные, относительно которых требуется сбор данных о трафике, и сведения об их связи с преступлением;

d) любые имеющиеся данные, идентифицирующие владельца или пользователя данных или местоположение информационно-коммуникационной системы;

e) обоснование необходимости сбора данных о трафике;

f) период, за который требуется собрать данные о трафике, и соответствующее обоснование его продолжительности.

Статья 46. Взаимная правовая помощь в перехвате данных о содержании

Государства-участники стремятся оказывать друг другу взаимную правовую помощь в сборе или записи в режиме реального времени данных о содержании, касающихся конкретных сообщений, передаваемых с помощью информационно-коммуникационной системы, в пределах, допускаемых применимыми к ним договорами или внутренним законодательством.

Статья 47. 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 противодействия преступлениям, признанным таковыми в соответствии с настоящей Конвенцией. Государства-участники, в частности, принимают эффективные меры, направленные на:

a) укрепление или, где это необходимо, установление каналов связи между их компетентными органами, учреждениями и службами с учетом существующих каналов, включая каналы Международной организации уголовной полиции, с целью обеспечить защищенный и быстрый обмен информацией обо всех аспектах преступлений, признанных таковыми в соответствии с 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, признанными таковыми в соответствии с настоящей Конвенцией, с целью выявления:

i) личности, местонахождения и деятельности лиц, подозреваемых в участии в совершении таких преступлений, или местонахождения других соответствующих лиц;

ii) перемещения доходов от преступлений или имущества, полученного в результате совершения таких преступлений;

iii) перемещения имущества, оборудования или других средств, использовавшихся или предназначавшихся для использования при совершении таких преступлений;

c) предоставление, в надлежащих случаях, необходимых предметов или данных для целей анализа или расследования;

d) обмен, в надлежащих случаях, с другими государствами-участниками информацией о конкретных средствах и методах, применяемых для совершения преступлений, признанных таковыми в соответствии с настоящей Конвенцией, включая использование ложных идентификационных данных, фальшивых, измененных или поддельных документов и других средств для сокрытия деятельности, а также о тактике, методах и процедурах киберпреступности;

e) содействие эффективной координации между их компетентными органами, учреждениями и службами и поощрение обмена сотрудниками и другими экспертами, включая направление сотрудников по связи в соответствии с двусторонними соглашениями или договоренностями между заинтересованными государствами-участниками;

f) обмен информацией и координацию административных и других мер, принимаемых в надлежащих случаях с целью заблаговременного выявления преступлений, признанных таковыми в соответствии с 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, внесения в них поправок. 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, признанных таковыми в соответствии с настоящей Конвенцией. В надлежащих случаях государства-участники в полной мере используют соглашения или договоренности, в том числе механизмы международных или ре-

гиональных организаций, для расширения сотрудничества между своими правоохранительными органами.

Статья 48. Совместные расследования

Государства-участники рассматривают возможность заключения двусторонних или многосторонних соглашений или договоренностей, на основании которых в связи с преступлениями, признанными таковыми в соответствии с настоящей Конвенцией и являющимися предметом уголовного расследования, преследования или судебного разбирательства в одном или нескольких государствах, заинтересованные компетентные органы могут создавать органы по проведению совместных расследований. В отсутствие таких соглашений или договоренностей совместные расследования могут проводиться по соглашению в каждом отдельном случае. Соответствующие государства-участники обеспечивают полное уважение суверенитета Государства-участника, на территории которого планируется провести такие расследования.

Статья 49. Механизмы возвращения имущества посредством международного сотрудничества в деле конфискации

1. Каждое Государство-участник в целях предоставления взаимной правовой помощи согласно статье 50 настоящей Конвенции в отношении имущества, приобретенного в результате совершения какого-либо из преступлений, признанных таковыми в соответствии с настоящей Конвенцией, или связанного с такими преступлениями, 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) принимает такие меры, какие могут потребоваться, с тем чтобы позволить своим компетентным органам, в пределах их юрисдикции, выносить постановления о конфискации такого имущества иностранного происхождения при вынесении судебных решений по делам об отмывании денежных средств или таким другим преступлениям, которые могут подпадать под его юрисдикцию, или при использовании других процедур, разрешенных его внутренним законодательством и

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 уголовному преследованию по причине смерти, побега или отсутствия либо в других соответствующих случаях.

2. Каждое Государство-участник в целях предоставления взаимной правовой помощи по просьбе, направленной согласно пункту 2 статьи 50 настоящей Конвенции, в соответствии со своим внутренним законодательством:

a) принимает такие меры, какие могут потребоваться, с тем чтобы позволить своим компетентным органам замораживать или налагать арест на имущество согласно постановлению о замораживании или аресте, которое вынесено судом или компетентным органом запрашивающего Государства-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 конечном итоге вынесено постановление о конфискации для целей подпункта (a) пункта 1 настоящей статьи;

b) принимает такие меры, какие могут потребоваться, с тем чтобы позволить своим компетентным органам замораживать или налагать арест на имущество в ответ на просьбу, в которой излагаются разумные основания, позволяющие запрашиваемому Государству-участнику полагать, что существуют достаточные мотивы для принятия таких мер и что в отношении этого имущества будет в конечном итоге вынесено постановление о конфискации для целей подпункта (a) пункта 1 настоящей статьи; и

c) рассматривает вопрос о принятии дополнительных мер, с тем чтобы позволить своим компетентным органам обеспечивать сохранность имущества для целей конфискации, например, на основании иностранного постановления об аресте или предъявления уголовного обвинения в связи с приобретением подобного имущества.

Статья 50. 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, просьбу о конфискации указанных в пункте 1 статьи 31 настоящей Конвенции доходов от преступлений, имущества, оборудования или других средств совершения преступлений, находящихся на его терри-

тории, в максимальной степени, возможной в рамках его внутренней правовой системы:

a) направляет эту просьбу своим компетентным органам с целью получения постановления о конфискации и, в случае вынесения такого постановления, приводит его в исполнение; или

b) направляет своим компетентным органам постановление о конфискации, вынесенное судом на территории запрашивающего Государства-участника в соответствии с пунктом 1 статьи 31 настоящей Конвенции, с целью исполнения в том объеме, который указан в просьбе, и в той мере, в какой оно относится к находящимся на территории запрашиваемого Государства-участника доходам от преступлений, имуществу, оборудованию или другим средствам совершения преступлений.

2. По получении просьбы, направленной другим Государством-участником, под юрисдикцию которого подпадает какое-либо преступление, признанное таковым в соответствии с настоящей Конвенцией, запрашиваемое Государство-участник принимает меры для выявления, отслеживания, замораживания или ареста доходов от преступлений, имущества, оборудования или других средств совершения преступлений, указанных в пункте 1 статьи 31 настоящей Конвенции, с целью последующей конфискации, постановление о которой выносится либо запрашивающим Государством-участником, либо, в соответствии с просьбой согласно пункту 1 настоящей статьи, запрашиваемым Государством-участником.

3. Положения статьи 40 настоящей Конвенции применяются mutatis mutandis к настоящей статье. В дополнение к информации, указанной в пункте 15 статьи 40 настоящей Конвенции, в просьбы, направляемые на основании настоящей статьи, включаются:

a) применительно к просьбе, предусмотренной в подпункте (a) пункта 1 настоящей статьи, — описание имущества, подлежащего конфискации, в том числе, насколько это возможно, сведения о местонахождении и, если это уместно, оценочная стоимость имущества и заявление с изложением фактов, на которые ссылается запрашивающее Государство-участник и которые достаточны для того, чтобы запрашиваемое Государство-участник могло принять меры для вынесения постановления согласно своему внутреннему законодательству;

b) применительно к просьбе, предусмотренной в подпункте (b) пункта 1 настоящей статьи, — выданная запрашивающим Государством-участником юридически допустимая копия постановления о конфискации, на котором основывается просьба, заявление с изложением фактов и информация в отношении объема запрашиваемого исполнения постановления, заявление, в котором указываются меры, принятые запрашивающим Государством-участником для обеспечения надлежащего уведомления добросовестных третьих сторон и соблюдения надлежащих правовых процедур, и заявление о том, что постановление о конфискации является окончательным;

c) применительно к просьбе, предусмотренной в пункте 2 настоящей статьи, — заявление с изложением фактов, на которые ссылается запрашивающее Государство-участник, и описание запрашиваемых мер, а также, при наличии таковой, юридически допустимая копия постановления, на котором основывается просьба.

4. Решения или меры, предусмотренные в пунктах 1 и 2 настоящей статьи, принимаются запрашиваемым Государством-участником в соответствии с положениями его внутреннего законодательства и его процессуальными нормами или любыми двусторонними или многосторонними договорами, соглашениями или договоренностями, которыми оно может быть связано в отношениях с запрашивающим Государством-участником, и при условии их соблюдения.

5. Каждое Государство-участник представляет Генеральному секретарю Организации Объединенных Наций тексты своих законов и правил, обеспечивающих осуществление положений настоящей статьи, а также тексты любых последующих изменений к таким законам и правилам или их описание.

6. Если какое-либо Государство-участник пожелает обусловить принятие мер, указанных в пунктах 1 и 2 настоящей статьи, наличием соответствующего договора, то это Государство-участник рассматривает настоящую Конвенцию в качестве необходимой и достаточной договорно-правовой основы.

7. В сотрудничестве согласно настоящей статье может быть также отказано или же обеспечительные меры могут быть сняты, если запрашиваемое Государство-участник не получает своевременно достаточных доказательств или если имущество имеет малую стоимость.

8. До снятия любой обеспечительной меры, принятой в соответствии с настоящей статьей, запрашиваемое Государство-участник, когда это возможно, предоставляет запрашивающему Государству-участнику возможность изложить свои мотивы в пользу продолжения осуществления такой меры.

9. Положения настоящей статьи не толкуются таким образом, чтобы наносился ущерб правам добросовестных третьих сторон.

10. Государства-участники рассматривают возможность заключения двусторонних или многосторонних договоров, соглашений или

договоренностей для повышения эффективности международного сотрудничества, осуществляемого согласно настоящей статье.

Статья 51. Специальное сотрудничество

Без ущерба для своего внутреннего законодательства каждое Государство-участник стремится принимать меры, позволяющие ему препровождать без ущерба для его собственного уголовного расследования, преследования или судебного разбирательства информацию о доходах от преступлений, признанных таковыми в соответствии с настоящей Конвенцией, другому Государству-участнику без предварительной просьбы, когда оно считает, что раскрытие такой информации может способствовать получающему ее Государству-участнику в возбуждении или проведении уголовного расследования, преследования или судебного разбирательства или может привести к направлению этим Государством-участником просьбы в соответствии со статьей 50 настоящей Конвенции.

Статья 52. Возвращение конфискованных доходов от преступлений или имущества и распоряжение ими

1. Доходами от преступлений или имуществом, конфискованными Государством-участником на основании статьи 31 или 50 настоящей Конвенции, распоряжается это Государство-участник в соответствии со своим внутренним законодательством и административными процедурами.

2. Действуя по просьбе, направленной другим Государством-участником в соответствии со статьей 50 настоящей Конвенции, государства-участники в той мере, в какой это допускается внутренним законодательством, и в случае получения соответствующей просьбы, в первоочередном порядке рассматривают вопрос о возвращении конфискованных доходов от преступлений или имущества запрашивающему Государству-участнику, с тем чтобы оно могло предоставить компенсацию потерпевшим от преступления или возвратить такие доходы от преступлений или имущество их прежним законным собственникам.

3. Действуя по просьбе, направленной другим Государством-участником в соответствии со статьями 31 и 50 настоящей Конвенции, Государство-участник может после надлежащего рассмотрения вопроса о компенсации потерпевшим особо рассмотреть возможность заключения соглашений или договоренностей:

a) о перечислении суммы, соответствующей стоимости доходов от преступлений или имущества, или средств, полученных в результате реализации таких доходов или имущества или их части, на счет, предназначенный для этой цели в соответствии с подпунктом (c) пункта 2 статьи 56 настоящей Конвенции, и межправительственным органам, специализирующимся на противодействии киберпреступности;

b) о передаче другим государствам-участникам на регулярной или разовой основе части доходов от преступлений или имущества, или средств, полученных в результате реализации таких доходов от преступлений или имущества, в соответствии со своим внутренним законодательством или административными процедурами.

4. В надлежащих случаях, если только государства-участники не примут иного решения, запрашиваемое Государство-участник может вычесть разумные расходы, понесенные в ходе расследования, преследования или судебного разбирательства, которые привели к возвращению конфискованного имущества или распоряжению им согласно настоящей статье.

Глава VI. Меры по предупреждению

Статья 53. Меры по предупреждению

1. Каждое Государство-участник стремится в соответствии с основополагающими принципами своей правовой системы разрабатывать и осуществлять или продолжать эффективную и скоординированную политику и передовую практику для сокращения существующих или будущих возможностей для совершения киберпреступлений посредством принятия надлежащих законодательных, административных или других мер.

2. Каждое Государство-участник принимает в пределах своих возможностей и в соответствии с основополагающими принципами своего внутреннего законодательства надлежащие меры для содействия активному участию соответствующих лиц и структур за пределами публичного сектора, таких как неправительственные организации, организации гражданского общества, научные учреждения и структуры частного сектора, и общественности в целом в соответствующих аспектах деятельности по предупреждению преступлений, признанных таковыми в соответствии с настоящей Конвенцией.

3. Меры по предупреждению могут включать:

a) укрепление сотрудничества между правоохранительными органами или прокурорами и соответствующими лицами и структурами за

пределами публичного сектора, такими как неправительственные организации, организации гражданского общества, научные учреждения и структуры частного сектора, в решении соответствующих аспектов проблемы предупреждения преступлений, признанных таковыми в соответствии с настоящей Конвенцией, и борьбы с ними;

b) содействие углублению понимания обществом факта существования, причин и опасного характера угрозы, создаваемой преступлениями, признанными таковыми в соответствии с настоящей Конвенцией, путем проведения информационной работы с населением и осуществления программ и учебных планов просвещения общественности и повышения уровня медийной и информационной грамотности, которые стимулируют участие общества в предупреждении таких преступлений и борьбе с ними;

c) создание и содействие укреплению потенциала национальных систем уголовного правосудия, включая организацию обучения и расширение экспертных знаний работников системы уголовного правосудия, в рамках национальных стратегий предупреждения преступлений, признанных таковыми в соответствии с настоящей Конвенцией;

d) стимулирование поставщиков услуг к принятию эффективных мер для усиления безопасности своих продуктов, услуг и клиентов, где это возможно с учетом национальных условий и в той мере, в какой это допускается внутренним законодательством;

e) признание вклада законной исследовательской деятельности в области безопасности, когда она направлена исключительно на усиление и повышение безопасности продуктов и услуг поставщиков и их клиентов, находящихся на территории Государства-участника, и в той мере, в какой это допускается внутренним законодательством, и при соблюдении установленных им условий;

f) разработку, содействие осуществлению и поддержку программ и мероприятий, преследующих цель удержать тех, кто может подвергнуться риску вовлечения в киберпреступность, от совершения преступлений и направить развитие их навыков в законное русло;

g) стремление содействовать реинтеграции в общество лиц, осужденных за преступления, признанные таковыми в соответствии с настоящей Конвенцией;

h) разработку, в соответствии с внутренним законодательством, стратегий и политики предотвращения и искоренения гендерного насилия, совершаемого с использованием информационно-коммуникационной системы, а также учет при разработке мер по предупреждению особых обстоятельств и потребностей лиц, находящихся в уязвимом положении;

i) принятие конкретных и адресных мер для обеспечения безопасности детей в интернет-пространстве, в том числе мер в области просвещения, подготовки кадров и повышения осведомленности общественности о сексуальных надругательствах над детьми или сексуальной эксплуатации детей в Интернете, и пересмотр национальной нормативно-правовой базы и укрепление международного сотрудничества с целью их предупреждения, а также принятие мер к обеспечению скорейшего удаления материалов со сценами сексуальных надругательств над детьми и сексуальной эксплуатации детей;

j) усиление прозрачности процессов принятия решений и содействие вовлечению населения в их принятие и обеспечение адекватной доступности информации для общественности;

k) уважение, поощрение и защиту свободы поиска, получения и распространения публичной информации, касающейся киберпреступности;

l) разработку или совершенствование программ поддержки потерпевших от преступлений, признанных таковыми в соответствии с настоящей Конвенцией;

m) предупреждение и выявление переводов доходов от преступлений и имущества, связанных с преступлениями, признанными таковыми в соответствии с настоящей Конвенцией.

4. Каждое Государство-участник принимает надлежащие меры к тому, чтобы соответствующий компетентный орган или органы, ответственные за предупреждение киберпреступности и борьбу с ней, были известны и доступны населению для направления им в надлежащих случаях сообщений, в том числе анонимных, о любых инцидентах, которые могут быть квалифицированы как уголовные правонарушения, признанные таковыми в соответствии с настоящей Конвенцией.

5. Государства-участники стремятся периодически проводить оценку соответствующего действующего национального законодательства и административной практики с целью выявления пробелов и слабых мест и обеспечения их актуальности перед лицом меняющихся угроз, которые создают правонарушения, признанные таковыми в соответствии с настоящей Конвенцией.

6. Государства-участники могут сотрудничать друг с другом и с соответствующими международными и региональными организациями в содействии осуществлению и разработке мер, указанных в настоя-

щей статье. Это включает участие в международных проектах, направленных на предупреждение киберпреступности.

7. 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 киберпреступности.

Глава VII. Техническая помощь и обмен информацией

Статья 54. Техническая помощь и наращивание потенциала

1. Государства-участники с учетом своих возможностей рассматривают вопрос об оказании друг другу самой широкой технической помощи и содействия в укреплении потенциала, включая подготовку кадров и другие формы помощи, взаимный обмен соответствующим опытом и специальными знаниями и передачу технологий на согласованных условиях с особым учетом интересов и потребностей развивающихся государств-участников с целью содействия предупреждению, выявлению и расследованию преступлений, охватываемых настоящей Конвенцией, и уголовному преследованию за них.

2. Государства-участники, насколько это необходимо, инициируют, разрабатывают, осуществляют или совершенствуют конкретные программы подготовки своего персонала, отвечающего за предупреждение, выявление и расследование преступлений, охватываемых настоящей Конвенцией, и уголовное преследование за них.

3. Виды деятельности, указанные в пунктах 1 и 2 настоящей статьи, могут охватывать, в той мере, в какой это допускается внутренним законодательством, следующие вопросы:

a) методы и приемы, используемые при предупреждении, выявлении и расследовании преступлений, охватываемых настоящей Конвенцией, и уголовном преследовании за них;

b) укрепление потенциала в области разработки и планирования стратегической политики и законодательства для предупреждения киберпреступности и борьбы с ней;

c) наращивание потенциала в области сбора, обеспечения сохранности и передачи доказательств, в частности в электронной форме, включая поддержание цепи обеспечения сохранности и проведение судебной экспертизы;

d) современное оборудование, предназначенное для правоохранительных органов, и его использование;

e) обучение сотрудников компетентных органов составлению просьб о взаимной правовой помощи и использованию других форм сотрудничества, удовлетворяющих требованиям настоящей Конвенции, особенно в части сбора, обеспечения сохранности и передачи доказательств в электронной форме;

f) предупреждение, выявление и мониторинг перемещения доходов, полученных в результате совершения преступлений, охватываемых настоящей Конвенцией, имущества, оборудования или других средств, а также методы, применяемые для перевода, сокрытия или утаивания таких доходов, имущества, оборудования или других средств;

g) надлежащие и действенные правовые и административные механизмы и методы, способствующие аресту, конфискации и возвращению доходов от преступлений, охватываемых настоящей Конвенцией;

h) методы защиты потерпевших и свидетелей, которые сотрудничают с судебными органами;

i) подготовка сотрудников по вопросам, касающимся соответствующих норм материального и процессуального права, полномочий правоохранительных органов при проведении расследований, а также национальных и международных правил, и изучение языков.

4. Государства-участники при условии соблюдения своего внутреннего законодательства стремятся использовать экспертные знания других государств-участников и соответствующих международных и региональных организаций, неправительственных организаций, организаций гражданского общества, научных учреждений и структур частного сектора и тесно сотрудничать с ними в целях повышения эффективности осуществления настоящей Конвенции.

5. Государства-участники оказывают друг другу содействие в планировании и осуществлении программ исследований и подготовки кадров для обеспечения обмена экспертными знаниями в областях, указанных в пункте 3 настоящей статьи, и с этой целью используют также, в надлежащих случаях, региональные и международные конференции и семинары для содействия сотрудничеству и обсуждению проблем, представляющих взаимный интерес.

6. Государства-участники рассматривают возможность оказания друг другу содействия, по просьбе, в проведении оценок, исследований и разработок, касающихся видов, причин и последствий охватываемых настоящей Конвенцией преступлений, совершенных на их соответствующих территориях, с целью разработки, с участием компетентных органов и соответствующих неправительственных организаций,

организаций гражданского общества, научных учреждений и структур частного сектора, стратегий и планов действий по предупреждению киберпреступности и борьбе с ней.

7. Государства-участники содействуют подготовке кадров и технической помощи, которая способствует своевременной выдаче и оказанию взаимной правовой помощи. Такая подготовка кадров и техническая помощь могут включать языковую подготовку, содействие в составлении и обработке просьб об оказании взаимной правовой помощи и командирование сотрудников центральных органов или учреждений, выполняющих соответствующие функции, и обмен такими сотрудниками.

8. Государства-участники активизируют, насколько это необходимо, усилия, направленные на максимальное повышение эффективности технической помощи и укрепления потенциала в международных и региональных организациях и в рамках соответствующих двусторонних и многосторонних соглашений или договоренностей.

9. Государства-участники рассматривают возможность создания добровольных механизмов для финансовой поддержки усилий развивающихся стран по осуществлению настоящей Конвенции посредством реализации программ технической помощи и проектов, направленных на укрепление потенциала.

10. Каждое Государство-участник стремится вносить добровольные взносы на нужды Управления Организации Объединенных Наций по наркотикам и преступности с целью содействия через Управление реализации программ и проектов для осуществления настоящей Конвенции посредством оказания технической помощи и укрепления потенциала.

Статья 55. Обмен информацией

1. Каждое государство-участник рассматривает возможность проведения в надлежащих случаях во взаимодействии с соответствующими экспертами, в том числе из неправительственных организаций, организаций гражданского общества, научных учреждений и структур частного сектора, анализа тенденций, характеризующих совершаемые на их территории преступления, охватываемые настоящей Конвенцией, а также обстоятельств, при которых совершаются такие преступления.

2. Государства-участники рассматривают возможность накопления статистических данных, аналитических знаний и информации о киберпреступлениях и обмена ими между собой и через посредство

международных и региональных организаций с целью выработки, насколько это возможно, общих определений, стандартов и методологий и оптимальных видов практики в деле предупреждения таких преступлений и борьбы с ними.

3. Каждое Государство-участник рассматривает возможность осуществления контроля за своей политикой и практическими мерами в области предупреждения преступлений, охватываемых настоящей Конвенцией, и борьбы с ними и проведения оценки их эффективности и действенности.

4. Государства-участники рассматривают возможность обмена информацией о правовых, политических и технологических изменениях, касающихся киберпреступности и сбора доказательств в электронной форме.

Статья 56. Осуществление Конвенции посредством экономического развития и технической помощи

1. Государства-участники принимают меры, способствующие оптимальному осуществлению настоящей Конвенции, насколько это возможно, посредством международного сотрудничества с учетом негативных последствий преступлений, охватываемых настоящей Конвенцией, для общества в целом и в частности для устойчивого развития.

2. Государствам-участникам настоятельно рекомендуется, насколько это возможно и в координации друг с другом, а также с международными и региональными организациями, предпринимать конкретные усилия для:

a) активизации своего сотрудничества на различных уровнях с другими государствами-участниками, особенно с развивающимися странами, в целях расширения их возможностей в области предупреждения преступлений, охватываемых настоящей Конвенцией, и борьбы с ними;

b) расширения финансовой и материальной помощи в целях поддержки усилий других государств-участников, в особенности усилий развивающихся стран, направленных на эффективное предупреждение преступлений, охватываемых настоящей Конвенцией, и борьбу с ними, и в целях оказания им содействия в осуществлении настоящей Конвенции;

c) оказания технической помощи другим государствам-участникам, в особенности развивающимся странам, в целях содействия удовлетворению их потребностей в связи с осуществлением настоящей Конвенции. Для этого государства-участники стремятся вносить на периоди-

ческой основе достаточные добровольные взносы на счет, предназначенный непосредственно для этой цели в механизме финансирования, созданном Организацией Объединенных Наций;

d) стимулирования в надлежащих случаях деятельности неправительственных организаций, организаций гражданского общества, научных учреждений и структур частного сектора, а также финансовых учреждений по поддержке усилий государств-участников, в том числе в соответствии с настоящей статьей, в частности путем увеличения количества программ подготовки кадров для развивающихся стран и предоставляемого им современного оборудования для содействия в достижении целей настоящей Конвенции;

e) обмена передовой практикой и информацией о проведенных мероприятиях с целью повышения прозрачности, избежания дублирования усилий и оптимального использования любых извлеченных уроков.

3. Государства-участники рассматривают также возможность использования существующих субрегиональных, региональных и международных программ, включая конференции и семинары, для содействия сотрудничеству и технической помощи и стимулирования обсуждения проблем, представляющих взаимный интерес, в том числе особых проблем и потребностей развивающихся стран.

4. Насколько это возможно, государства-участники обеспечивают распределение и направление ресурсов и усилий на содействие согласованию стандартов, навыков, потенциала, экспертных знаний и технических возможностей с целью установления общих минимальных стандартов среди государств-участников для ликвидации условий, позволяющих безнаказанно совершать преступления, охватываемые настоящей Конвенцией, и усиления противодействия киберпреступности.

5. Насколько это возможно, меры, принятые в соответствии с настоящей статьей, не затрагивают существующие обязательства в отношении иностранной помощи или другие договоренности о финансовом сотрудничестве на двустороннем, региональном или международном уровне.

6. Государства-участники могут заключать двусторонние, региональные или многосторонние соглашения или договоренности о материально-технической помощи, принимая во внимание финансовые договоренности, необходимые для обеспечения эффективности международного сотрудничества, предусмотренного настоящей Конвенцией, а также для предупреждения, выявления и расследования преступлений, охватываемых настоящей Конвенцией, и уголовного преследования за них.

Глава VIII. Механизм осуществления

Статья 57. 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 осуществлению настоящей Конвенции и проведения обзора хода ее осуществления.

2. Генеральный секретарь Организации Объединенных Наций созывает Конференцию государств-участников не позднее чем через один год после вступления настоящей Конвенции в силу. Впоследствии в соответствии с правилами процедуры, принятыми Конференцией, проводятся очередные совещания 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. В таких правилах и соответствующей деятельности учитываются такие принципы, как эффективность, всеохватность, прозрачность, результативность и национальная ответственность.

4. При назначении своих очередных совещаний Конференция государств-участников принимает во внимание время и место проведения совещаний других соответствующих международных и региональных организаций и механизмов по аналогичным вопросам, включая их вспомогательные договорные органы, в соответствии с принципами, определенными в пункте 3 настоящей статьи.

5. Конференция государств-участников согласовывает виды деятельности, процедуры и методы работы для достижения целей, изложенных в пункте 1 настоящей статьи, включая:

a) содействие эффективному использованию и осуществлению настоящей Конвенции и выявлению любых связанных с ней проблем, а также деятельности, осуществляемой государствами-участниками в рамках настоящей Конвенции, включая поощрение мобилизации добровольных взносов;

b) содействие обмену информацией о правовых, политических и технологических изменениях, касающихся преступлений, признанных таковыми в соответствии с настоящей Конвенцией, и сбора доказательств в электронной форме, между государствами-участниками и соответствующими международными и региональными организациями,

а также неправительственными организациями, организациями гражданского общества, научными учреждениями и структурами частного сектора в соответствии с внутренним законодательством, а также информацией о закономерностях и тенденциях киберпреступности и успешных методах предупреждения указанных преступлений и борьбы с ними;

c) сотрудничество с соответствующими международными и региональными организациями, а также неправительственными организациями, организациями гражданского общества, научными учреждениями и структурами частного сектора;

d) надлежащее использование соответствующей информации, подготовленной другими международными и региональными организациями и механизмами в целях предупреждения преступлений, признанных таковыми в соответствии с настоящей Конвенцией, и борьбы с ними, во избежание излишнего дублирования работы;

e) периодическое рассмотрение вопроса об осуществлении настоящей Конвенции ее государствами-участниками;

f) вынесение рекомендаций, касающихся совершенствования настоящей Конвенции и ее осуществления, а также рассмотрение возможных дополнений или поправок к Конвенции;

g) разработку и принятие дополнительных протоколов к настоящей Конвенции в соответствии со статьями 61 и 62 настоящей Конвенции;

h) учет потребностей государств-участников в технической помощи и укреплении потенциала в связи с осуществлением настоящей Конвенции и вынесение рекомендаций в отношении любых действий, которые она может считать необходимыми в связи с этим.

6. Каждое Государство-участник представляет Конференции государств-участников информацию о законодательных, административных и иных мерах, а также о своих программах, планах и практике, направленных на осуществление настоящей Конвенции, как это требуется Конференции. Конференция 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 и региональных организаций. Могут быть рассмотрены также материалы, полученные от представителей соответствующих неправительственных организаций, организаций гражданского общества, научных учреждений и структур частного сектора, надлежащим образом аккредитованных в соответствии с процедурами, которые будут определены решением Конференции.

7. Для целей пункта 5 настоящей статьи Конференция государств-участников может создавать такие механизмы обзора, которые она считает необходимыми, и управлять ими.

8. Согласно пунктам 5—7 настоящей статьи Конференция государств-участников, если она сочтет это необходимым, учреждает любые соответствующие механизмы или вспомогательные органы для содействия эффективному осуществлению Конвенции.

Статья 58. Секретариат

1. Генеральный секретарь Организации Объединенных Наций обеспечивает необходимое секретариатское обслуживание Конференции государств — участников Конвенции.

2. Секретариат:

a) оказывает Конференции государств-участников помощь в осуществлении деятельности, о которой говорится в настоящей Конвенции, а также организует сессии Конференции, имеющие отношение к настоящей Конвенции, и обеспечивает их необходимым обслуживанием;

b) оказывает государствам-участникам по их просьбе помощь в предоставлении информации Конференции государств-участников, как это предусмотрено в настоящей Конвенции; и

c) обеспечивает необходимую координацию с секретариатами соответствующих международных и региональных организаций.

Глава IX. Заключительные положения

Статья 59. Осуществление Конвенции

1. Каждое Государство-участник принимает, в соответствии с основополагающими принципами своего внутреннего законодательства, необходимые меры, включая законодательные и административные меры, для обеспечения осуществления своих обязательств согласно настоящей Конвенции.

2. Каждое Государство-участник может принимать более строгие или суровые меры, чем меры, предусмотренные настоящей Конвенцией, для предупреждения преступлений, признанных таковыми в соответствии с настоящей Конвенцией, и борьбы с ними.

Статья 60. Действие Конвенции

1. Если два или более государства-участника уже заключили соглашение или договор по вопросам, рассматриваемым в настоящей Кон-

венции, или иным образом установили свои отношения по таким вопросам либо если они сделают это в будущем, они имеют также право применять это соглашение или договор либо регулировать эти отношения соответствующим образом.

2. Ничто в настоящей Конвенции не затрагивает других прав, ограничений, обязательств и обязанностей Государства-участника согласно международному праву.

Статья 61. Взаимосвязь с протоколами

1. Настоящая Конвенция может быть дополнена одним или несколькими протоколами.

2. Для того чтобы стать Участником протокола, государство или региональная организация экономической интеграции должны быть также Участником настоящей Конвенции.

3. Государство — участник настоящей Конвенции не связано протоколом, если только оно не становится Участником протокола в соответствии с его положениями.

4. Любой протокол к настоящей Конвенции толкуется совместно с настоящей Конвенцией с учетом цели этого протокола.

Статья 62. Принятие дополнительных протоколов

1. Для того чтобы любой дополнительный протокол был рассмотрен на предмет принятия Конференцией государств-участников, требуется не менее 60 государств-участников. Конференция прилагает все усилия для достижения консенсуса в отношении любого дополнительного протокола. Если все возможности для достижения консенсуса были исчерпаны и согласие достигнуто не было, то в качестве последнего средства для принятия дополнительного протокола устанавливается требование о большинстве, составляющем не менее двух третей голосов государств-участников, присутствующих и участвующих в голосовании на заседании Конференции.

2. В вопросах, входящих в сферу компетенции региональных организаций экономической интеграции, они осуществляют свое право голоса согласно настоящей статье, располагая числом голосов, равным числу их государств-членов, являющихся участниками настоящей Конвенции. Такие организации не осуществляют свое право голоса, если их государства-члены осуществляют собственное право голоса, и наоборот.

Статья 63. Урегулирование споров

1. Государства-участники стремятся урегулировать споры относительно толкования или применения настоящей Конвенции путем переговоров или любым иным мирным способом по своему выбору.

2. Любой спор между двумя или более государствами-участниками относительно толкования или применения настоящей Конвенции, который не может быть урегулирован путем переговоров или иными мирными средствами в течение разумного периода времени, передается по просьбе одного из этих государств-участников на арбитражное разбирательство. Если в течение шести месяцев со дня обращения с просьбой об арбитраже эти государства-участники не смогут договориться о его организации, любое из этих государств-участников может передать спор в Международный Суд, обратившись с заявлением в соответствии со Статутом Суда.

3. Каждое Государство-участник может при подписании, ратификации, принятии или утверждении настоящей Конвенции или при присоединении к ней заявить о том, что оно не считает себя связанным положениями пункта 2 настоящей статьи. Другие государства-участники не связаны положениями пункта 2 настоящей статьи в отношении любого Государства-участника, сделавшего такую оговорку.

4. Любое Государство-участник, сделавшее оговорку в соответствии с пунктом 3 настоящей статьи, может в любое время снять эту оговорку путем направления уведомления Генеральному секретарю Организации Объединенных Наций.

Статья 64. Подписание, ратификация, принятие, утверждение и присоединение

1. Настоящая Конвенция открыта для подписания всеми государствами в Ханое в 2025 году, а затем в Центральных учреждениях Организации Объединенных Наций в Нью-Йорке до 31 декабря 2026 года.

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. Ратификационные грамоты или документы о принятии или утверждении сдаются на хранение Генеральному секретарю

Организации Объединенных Наций. Региональная организация экономической интеграции может сдать на хранение свою ратификационную грамоту или документ о принятии или утверждении, если по меньшей мере одно из ее государств-членов поступило таким же образом. В этой ратификационной грамоте или документе о принятии или утверждении 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.

4. Настоящая Конвенция открыта для присоединения любого государства или любой региональной организации экономической интеграции, по меньшей мере одно из государств-членов которой является Участником настоящей Конвенции. Документы о присоединении сдаются на хранение Генеральному секретарю Организации Объединенных Наций. При присоединении региональная организация экономической интеграции заявляет о сфере своей компетенции в отношении вопросов, регулируемых настоящей Конвенцией. Такая организация также сообщает депозитарию о любом соответствующем изменении сферы своей компетенции.

Статья 65. Вступление в силу

1. Настоящая Конвенция вступает в силу на девяностый день после даты сдачи на хранение сороковой ратификационной грамоты или документа о принятии, утверждении или присоединении. Для цели настоящего пункта любая такая грамота или документ, сданные на хранение региональной организацией экономической интеграции, не рассматриваются в качестве дополнительных к грамотам или документам, сданным на хранение государствами — членами этой организации.

2. Для каждого государства или региональной организации экономической интеграции, которые ратифицируют, принимают, утверждают настоящую Конвенцию или присоединяются к ней после сдачи на хранение сороковой ратификационной грамоты или документа о таком действии, настоящая Конвенция вступает в силу на тридцатый день после даты сдачи на хранение таким государством или организацией соответствующей грамоты или документа или в дату вступления настоящей Конвенции в силу в соответствии с пунктом 1 настоящей статьи, в зависимости от того, что наступает позднее.

Статья 66. Поправки

1. По истечении пяти 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 прилагает все усилия для достижения консенсуса в отношении каждой поправки. Если все возможности для достижения консенсуса были исчерпаны и согласие достигнуто не было, то в качестве последнего средства для принятия поправки устанавливается требование о большинстве, составляющем две трети голосов государств-участников, присутствующих и участвующих в голосовании на заседании Конференции.

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, являющихся Участниками настоящей Конвенции. 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.

4. Поправка, принятая в соответствии с пунктом 1 настоящей статьи, вступает в силу в отношении Государства-участника через 90 дней после даты сдачи им на хранение Генеральному секретарю Организации Объединенных Наций ратификационной грамоты или документа о принятии или утверждении такой поправки.

5. Когда поправка вступает в силу, она становится обязательной для тех государств-участников, которые выразили согласие быть связанными ею. Другие государства-участники продолжают быть связанными положениями настоящей Конвенции и любыми поправками, ратифицированными, принятыми или утвержденными ими ранее.

Статья 67. Денонсация

1. Государство-участник может денонсировать настоящую Конвенцию путем направления письменного уведомления Генеральному секретарю Организации Объединенных Наций. Такая денонсация всту-

пает в силу по истечении одного года после даты получения уведомления Генеральным секретарем.

2. Региональная организация экономической интеграции перестает быть Участником настоящей Конвенции, когда все ее государства-члены денонсировали настоящую Конвенцию.

3. Денонсация настоящей Конвенции в соответствии с пунктом 1 настоящей статьи влечет за собой денонсацию любых протоколов к ней.

Статья 68. 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[1].

Примечания для толкования по конкретным статьям Конвенции Организации Объединенных Наций против киберпреступности; укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям

Статья 2

1. В определение термина «поставщик услуг» в подпункте (e)(ii) статьи 2 включены те организации, которые хранят или иным образом обрабатывают электронные данные от имени пользователей услуг, указанных в подпункте (i). Например, согласно этому определению,

[1] Специальный комитет по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях представил примечания для толкования по статьям 2, 17, 23 и 35 настоящей Конвенции в приложении к докладу о работе его возобновленной заключительной сессии, состоявшейся 29 июля — 9 августа 2024 г. в Нью-Йорке.

к поставщикам услуг относятся как структуры, обеспечивающие хостинг и кеширование, так и структуры, обеспечивающие подключение к сети. При этом лица, которые просто пользуются услугами хостинговой компании для размещения своих сайтов, не подпадают под это определение.

2. Государства-участники не обязаны дословно воспроизводить в своем внутреннем законодательстве те же термины, определения которых даны в статье 2 Конвенции, при условии, что их законодательство охватывает эти понятия таким образом, что это соответствует принципам и целям Конвенции и обеспечивает эквивалентные рамки для ее осуществления.

Статья 17

3. В рамках Конвенции правонарушение считается правонарушением в соответствии со статьей 17 только в том случае, если основным правонарушением является правонарушение, признанное таковым в соответствии со статьями 7—16 Конвенции.

Статьи 23 и 35 — относительно термина «расследование»

4. Под «уголовными расследованиями» понимаются ситуации, когда фактические обстоятельства дают разумные основания полагать, что совершено или совершается уголовное правонарушение (включая правонарушение, предусмотренное в статье 19 Конвенции), в том числе когда расследование направлено на то, чтобы остановить соответствующее преступление или воспрепятствовать его совершению.

Статья 35

5. Вне рамок Конвенции государства-участники могут осуществлять международное сотрудничество друг с другом в соответствии со своими международными обязательствами в любых других формах, допускаемых внутренним законодательством запрашиваемого государства-участника, применимыми договорами о взаимной правовой помощи или эквивалентными договоренностями[1].

[1] О вкладе Российской Федерации в разработку принятой Конвенции ООН см.: *Пузырева Ю. В., Бардина Е. Е., Мысина А. И.* и др. Противодействие использованию информационно-коммуникационных технологий в преступных целях. Приоритеты международного сотрудничества РФ. М., 2024. (*Примеч. сост.*)

Приложение 2

Концепция государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий, утвержденная распоряжением Правительства Российской Федерации от 30 декабря 2024 г. № 4154-р

I. Общие положения

Настоящая Концепция определяет принципы, цели, задачи и функции государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий, а также нормативно-правовое, научно-техническое, информационно-аналитическое, кадровое, организационно-штатное и финансовое обеспечение ее создания и функционирования.

Правовую основу настоящей Концепции составляют Конституция Российской Федерации, федеральные законы «О стратегическом планировании в Российской Федерации», «Об основах системы профилактики правонарушений в Российской Федерации», «Об информации, информационных технологиях и о защите информации», указы Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации», от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017—2030 годы», от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации», от 7 мая 2024 г. № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» и иные нормативные правовые акты Российской Федерации.

Для целей реализации настоящей Концепции используются следующие основные понятия:

«государственная система противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий» (далее — государственная система) — совокупность федеральных государственных органов и органов государственной власти субъектов Российской Федерации, осуществляющих при участии Центрального банка Российской Федерации, финансовых и иных организаций функции по выработке и реализации государственной политики в сфере противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий, а также разработку государственных требований и правил различного уровня и направленности в указанной сфере, созданных ими консультативных, совещательных и иных органов, а также организаций, деятельность которых связана со сбором, хранением персональных данных, созданием и функционированием информационной инфраструктуры, оборотом цифровой валюты, организаций, предоставляющих услуги связи и доступа к информационно-телекоммуникационной сети «Интернет» (далее — сеть «Интернет»), потребителей указанных услуг, институтов гражданского общества, объектов информационной инфраструктуры;

«информационно-коммуникационная сфера» — совокупность информационно-телекоммуникационных сетей, включая сеть «Интернет», технологической инфраструктуры, обеспечивающей их функционирование, и различных форм человеческой активности, осуществляемой посредством их использования;

«информационно-коммуникационные технологии» — процессы и методы создания, обработки, распространения информации, а также способы и средства их осуществления;

«противоправные деяния, совершенные с использованием информационно-коммуникационных технологий» (далее — противоправные деяния) — общественно опасные деяния, за которые предусмотрена уголовная либо административная ответственность, совершенные с использованием (применением) информационно-коммуникационных технологий или в сфере компьютерной информации, в том числе с использованием (применением) электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет», информационной инфраструктуры, компьютерной техники, программных средств, онлайн-сервисов, средств коммуникации (в том числе средств мобильной связи, сервисов обмена мгновенными сообщениями, IP-телефонии), электронных средств платежа, операций с цифровой валютой и цифровыми финансовыми активами;

«средства государственной системы» — технологии, аппаратно-программные, организационные и другие средства сбора, хранения и анализа информации, предназначенные для противодействия противоправным деяниям.

Противоправные деяния с учетом критериев их квалификации классифицируются по трем основным типам:

правонарушения и преступления в сфере компьютерной информации;

правонарушения и преступления, криминообразующим или квалифицирующим признаком которых является их совершение с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»;

правонарушения и преступления, при совершении которых применение информационно-коммуникационных технологий является альтернативным способом.

Назначением государственной системы является обеспечение проведения единой государственной политики по противодействию противоправным деяниям, направленной на защиту основных прав и свобод человека и гражданина и обеспечение национальной безопасности Российской Федерации в цифровой среде.

Создание и функционирование государственной системы осуществляется на основе следующих принципов:

гарантированности конституционных прав и свобод человека и гражданина при профилактике и противодействии противоправным деяниям;

обеспечения безопасности личности, общества и государства при противодействии противоправным деяниям;

единства государственного планирования, а также координации и контроля реализации комплекса технических и организационных мер;

рациональности использования сил и средств государственной системы.

II. Современное состояние противодействия противоправным деяниям

В Российской Федерации информационное общество характеризуется широким распространением и доступностью мобильных устройств, а также беспроводных технологий и сетей связи.

Пользователями российского сегмента сети «Интернет» в 2024 году стали более 130 млн человек, что составляет около 90 процентов населения страны, активными пользователями социальных сетей — 106 млн человек, или более 81 процента от всех российских пользователей сети «Интернет». Электронные средства массовой информации, информационные системы, социальные сети сегодня являются частью повседневной жизни россиян. Создана система предоставления государственных и муниципальных услуг в электронной форме.

Информационно-коммуникационные технологии стали частью современных управленческих систем практически во всех сферах жизни

российского общества. Развитие инструментов финансового рынка, платежных систем, а также в целом цифровизация экономических процессов дали толчок к появлению специфических способов расчетов — электронных средств платежа и их использованию юридическими и физическими лицами для безналичных расчетов.

Бесконтрольный оборот электронных средств платежа после их получения от кредитных организаций, создающий условия для их последующего использования в целях совершения незаконных действий, несет общественную опасность.

Учитывая, что в Российской Федерации сформировалось информационное общество, в котором информация и уровень ее применения и доступности кардинальным образом влияют на экономические и социокультурные условия жизни граждан, злоумышленники также перестроились на совершение преступлений в информационном пространстве.

Преступные посягательства в информационно-коммуникационной сфере с каждым годом занимают все более заметное место в структуре всех зарегистрированных преступлений в стране. За последние пять лет количество таких преступлений возросло более чем в два раза (с 294,4 тыс. преступлений в 2019 году до 677 тыс. в 2023 году). Также вырос их удельный вес в числе всех зарегистрированных деяний (с 14,5 процента в 2019 году до 34,8 процента в 2023 году). В настоящее время практически каждое третье преступление совершено в информационно-коммуникационной сфере либо с использованием информационно-коммуникационных технологий.

В структуре преступлений данной категории в 2023 году преобладали кражи и мошенничества, которые составили почти три четверти таких преступлений (70,2 процента). Каждое восьмое преступление (12 процентов) совершалось с целью незаконного производства, сбыта или пересылки наркотических средств и психотропных веществ. Экономическую направленность имеют 3,4 процента преступлений, экстремистскую направленность и террористический характер — 0,2 процента.

Также отмечается существенное увеличение количества преступлений, связанных с неправомерным доступом к компьютерной информации, их доля в общем числе преступлений, совершаемых с использованием информационно-коммуникационных технологий, по итогам 2023 года возросла в 6,8 раза. При этом раскрываемость таких преступлений остается на крайне низком уровне (5,6 процента).

Противоправные деяния, связанные с неправомерным доступом к компьютерной информации, как правило, сопровождаются утечками конфиденциальных сведений, что может нанести ущерб как отдельным лицам, так и организациям, функционирующим в том числе в сфере оборонно-промышленного комплекса и смежных отраслях промышленности. В связи с этим необходимо создание надежного барьера противодействия посягательствам в данной сфере.

В противоправном применении информационно-коммуникационных технологий особую активность проявляют организованные преступные группы. Они используют вредоносное программное обеспечение, фишинговые сайты, специальную технику, электронные платформы и колл-центры для совершения массовых мошеннических звонков.

Анализ совершенных противоправных деяний показывает, что все более широкое распространение получают хищения кредитных денежных средств, полученных как самими потерпевшими под непосредственным влиянием злоумышленников, так и в результате доступа преступников к системам дистанционного банковского обслуживания или регистрации на сайтах микрофинансовых организаций под учетными записями граждан.

Подходы к организации дистанционного банковского обслуживания нуждаются в адаптации в целях устранения уязвимостей и минимизации возможного ущерба при оказании услуг как для граждан, так и для самих кредитных организаций. Выводу на рынок связи новых видов услуг (IP-телефония, виртуальные автоматические телефонные станции) должна предшествовать их нормативная регламентация в целях снижения рисков анонимизации фактического потребителя.

Существенное негативное влияние на криминогенную обстановку в информационно-коммуникационной сфере оказывает сложная международная ситуация, в том числе связанная с деятельностью спецслужб недружественных государств и неонацистских формирований, курируемых иностранными спецслужбами. Основная масса преступлений совершается специализирующимися на мошенничествах транснациональными организованными преступными группами, связанными с организацией хищения персональных данных граждан Российской Федерации и работой действующих с территорий недружественных государств колл-центров, с использованием которых похищаются средства граждан.

Международные преступные группы и сообщества ввиду трансграничного характера информационного пространства и отсутствия

должного уровня межгосударственного взаимодействия успешно используют имеющиеся в настоящее время уязвимости в нормативно-правовом и организационно-техническом обеспечении противодействия противоправным деяниям, нанося существенный материальный и репутационный вред гражданам и организациям Российской Федерации.

Все большее распространение получает использование цифровой валюты при совершении преступлений, особенно при отмывании преступных доходов, поскольку это позволяет скрыть источник происхождения средств и конечного бенефициара — их получателя, что фактически исключает возможность выявления и конфискации использовавшейся при совершении экономических преступлений цифровой валюты.

Рост числа противоправных деяний обусловлен не только активным развитием самих информационно-коммуникационных технологий, но и виктимным поведением потерпевших, в том числе низким уровнем правовой и финансовой грамотности граждан, применением новых способов совершения противоправных деяний, наличием условий для обеспечения анонимности преступников. Несмотря на принимаемые органами государственной власти меры, направленные на борьбу с преступными и иными противоправными посягательствами, необходимый уровень информационной безопасности не достигнут.

Ситуация, складывающаяся при взаимодействии правоохранительных органов с операторами связи, провайдерами хостинга, организаторами распространения информации и иными субъектами информационного обмена, свидетельствует о необходимости адаптации бизнес-моделей предоставления услуг потребителям в сети «Интернет» с учетом рисков криминального использования информационно-коммуникационных технологий, в том числе связанных с неправомерным или случайным доступом к персональным данным, их уничтожением, изменением, блокированием, копированием, предоставлением, распространением, а также иными неправомерными действиями в отношении персональных данных. Существенным фактором, влияющим на эффективность противодействия противоправным деяниям, является отсутствие механизма обмена в режиме реального времени информацией между указанными организациями и правоохранительными органами, в том числе обеспечивающего передачу документов распорядительного (обязательного к исполнению) характера и конфиденциальной информации.

Предупреждение и пресечение правонарушений и преступлений, совершаемых с использованием информационно-коммуникационных технологий, в том числе легализации преступных доходов, финансирования терроризма, организации незаконного распространения наркотических средств и психотропных веществ, а также использования в противоправных целях цифровых валют определены Стратегией национальной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации», как одни из основных задач достижения целей обеспечения государственной и общественной безопасности.

Обеспечение и защита конституционных прав и свобод человека и гражданина в части, касающейся получения и использования информации и неприкосновенности частной жизни при использовании информационных технологий, отнесены к национальным интересам Российской Федерации в информационной сфере согласно Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».

Для повышения эффективности противодействия противоправным деяниям требуются согласованные действия федеральных государственных органов и органов государственной власти субъектов Российской Федерации, а также их взаимодействие с Центральным банком Российской Федерации, финансовыми и иными организациями, институтами гражданского общества.

III. Цель, задачи и функции государственной системы

Целью государственной системы является защита государства, общества и граждан от противоправных деяний.

Основными задачами государственной системы являются:

прогнозирование противоправных деяний; выявление противоправных деяний;

повышение результативности расследования преступлений, совершаемых с использованием информационно-коммуникационных технологий;

совершенствование законодательства в сфере противодействия противоправным деяниям;

разработка и реализация правовых, организационных, технических и иных мер противодействия противоправным деяниям;

сбор, обработка, анализ и обмен информацией в сфере противодействия противоправным деяниям;

совершенствование инструментов и механизмов противодействия преступлениям и правонарушениям, совершаемым с использованием информационно-коммуникационных технологий;

создание подразделений, специализирующихся на противодействии противоправным деяниям;

обеспечение защищенности российского общества от противоправных посягательств в информационном пространстве, включая обеспечение безопасности персональных данных;

содействие восстановлению имущественных и иных прав граждан, нарушенных в результате совершенных в отношении их противоправных деяний, оказание им правовой и психологической помощи;

обеспечение на системной основе максимально широкого информирования населения о новых приемах совершения противоправных деяний и способах противодействия им;

развитие цифровой грамотности населения, правосознания граждан и их ответственного отношения к использованию информационно-коммуникационных технологий, в том числе потребительской и пользовательской культуры, культуры поведения в цифровом пространстве, а также содействие активному применению программно-технических средств защиты от противоправных деяний;

укрепление международного сотрудничества в сфере противодействия противоправным деяниям.

Для выполнения основных задач государственная система осуществляет реализацию следующих функций:

создание специализированной цифровой платформы, обеспечивающей оперативный обмен информацией между правоохранительными органами, Центральным банком Российской Федерации, кредитными организациями, а также операторами связи о сведениях, необходимых для установления обстоятельств противоправных деяний и лиц, их совершивших, с использованием средств мобильной связи, сервисов сети «Интернет» и иных информационных технологий (за исключением компьютерных атак и компьютерных инцидентов);

формирование и поддержание в актуальном состоянии информационных ресурсов федеральных государственных органов и органов государственной власти субъектов Российской Федерации, осуществляющих выработку и реализацию государственной политики в сфере противодействия противоправным деяниям, организаций, деятельность которых связана со сбором, хранением персональных данных, созда-

нием и функционированием информационной инфраструктуры, оборотом цифровой валюты, кредитно-финансовых организаций, организаций, предоставляющих услуги связи и доступа к сети «Интернет»;

проведение мониторинга и ограничение доступа к противоправным ресурсам в информационно-телекоммуникационных сетях, включая сеть «Интернет»;

обеспечение эффективного применения норм законодательства Российской Федерации в сфере противодействия противоправным деяниям, в том числе проведение систематического мониторинга правоприменительной практики в данной сфере;

адаптация законодательства Российской Федерации под новые реалии в целях регулирования порядка оказания услуг, при котором риски их предоставления в условиях анонимизации будут полностью исключены, за нарушение порядка оказания государственных услуг введена соответствующая ответственность, а также совершенствование законодательства Российской Федерации в части организации электронного обмена данными кредитно-финансовых учреждений с органами государственной власти;

принятие на региональном и муниципальном уровнях соответствующих целевых программ, предусматривающих формирование системы профилактики правонарушений и преступлений, совершаемых с использованием информационно-коммуникационных технологий;

совершенствование вопросов, связанных с порядком выпуска, обращения и реализации ограничительных процедур в отношении цифровой валюты;

реализация механизма оперативного приостановления операций с денежными средствами, электронными денежными средствами, авансовыми платежами за услуги связи, использовавшимися в преступной деятельности;

формирование у бизнес-сообщества приоритета при предоставлении услуг на соблюдение прав потребителя и обеспечение его безопасности;

оказание содействия средствам массовой информации в широком и объективном освещении деятельности государственной системы;

повышение уровня международного сотрудничества и использование накопленного международного опыта в целях противодействия противоправным деяниям;

организация и проведение научно-исследовательских и опытно-конструкторских работ по разработке и применению криминалистических средств и методов выявления, раскрытия и расследования преступлений, совершаемых с использованием информационно-коммуникационных технологий, а также сбора доказательств;

расширение практики привлечения экспертного и научного сообществ при подготовке проектов нормативных документов в сфере противодействия противоправным деяниям;

повышение уровня материального и технического оснащения федеральных государственных органов и органов государственной власти субъектов Российской Федерации, осуществляющих функции по выработке и реализации государственной политики в сфере противодействия противоправным деяниям, а также уровня правовой и социальной защищенности их сотрудников, включая обеспечение правовой защиты сотрудников правоохранительных и следственных органов, специалистов, экспертов, использующих в своей деятельности методы, сопряженные с нарушением личной, банковской и иной охраняемой федеральными законами тайны;

организация мероприятий по повышению квалификации сотрудников и работников федеральных государственных органов, органов государственной власти субъектов Российской Федерации, финансовых и иных организаций, участвующих в противодействии противоправным деяниям;

совершенствование уголовного законодательства в части определения видов преступлений, совершенных с использованием информационно-коммуникационных технологий, а также государственной статистической отчетности о таких преступлениях;

совершенствование профилактических мер по снижению доли несовершеннолетних, вовлеченных в противоправную деятельность в информационно-коммуникационной сфере;

повышение уровня осведомленности граждан, в первую очередь пожилых, о методах совершения противоправных деяний и способах защиты от них, подготовка и размещение социальной рекламы, направленной на воспитание у граждан цифровой грамотности, с привлечением к этой деятельности представителей культуры, науки, общественности и информационного сообщества;

выстраивание эффективного международного сотрудничества с правоохранительными органами, финансовыми и иными организациями иностранных государств по противодействию противоправным деяниям с учетом необходимости преодоления двойных стандартов в подходах зарубежных партнеров к уголовному преследованию лиц, совершивших преступления, а также адекватного использования имеющихся международных правовых инструментов.

IV. Нормативно-правовое, научно-техническое, информационно-аналитическое, кадровое, организационно-штатное и финансовое обеспечение создания и функционирования государственной системы

Нормативно-правовое обеспечение создания и функционирования государственной системы включает в себя:

подготовку и принятие соответствующих правовых актов, направленных на повышение эффективности деятельности государственной системы, в том числе в части фиксации и обмена соответствующей информацией;

документы стратегического планирования, разработанные на федеральном и региональном уровнях; порядок осуществления деятельности участников государственной системы;

порядок и периодичность проведения мероприятий по оценке степени защищенности российского общества от противоправных деяний.

Нормативно-правовая база противодействия противоправным деяниям должна соответствовать следующим требованиям:

совершенствование с учетом появления новых способов и форм совершения преступлений и правонарушений;

определение компетенции участников государственной системы;

учет международного опыта, реальных системообразующих, социальных, экономических и других модернизирующих факторов;

установление ответственности физических и юридических лиц за несоблюдение требований законодательства Российской Федерации в области противодействия противоправным деяниям;

обеспечение эффективности административного и уголовного преследования за преступления и правонарушения, совершаемые с использованием информационно-коммуникационных технологий.

Научно-техническое обеспечение создания и функционирования государственной системы включает в себя:

разработку теоретических и методологических основ противодействия преступлениям и правонарушениям, совершаемым с использованием информационно-коммуникационных технологий, рекомендаций для решения практических задач по конкретным направлениям деятельности, включая обеспечение оперативно-разыскных и иных мероприятий (контроль за условно осужденными, лицами находящимися под административным надзором, мигрантами и др.), а также специальные и экспертные исследования в области противодействия противоправным деяниям;

проведение прикладных научных исследований для принятия правовых, организационных и управленческих решений в области противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий, на разных уровнях;

изучение и анализ международного опыта противодействия противоправным деяниям, внесение заинтересованными государственными органами предложений по совершенствованию мер борьбы с противоправными деяниями;

исследование основных факторов, определяющих сущность и актуальное состояние противодействия преступлениям и правонарушениям, совершаемым с использованием информационно-коммуникационных технологий;

анализ информации о политических, социально-экономических и иных общественных процессах в Российской Федерации и мире, оказывающих негативное влияние на криминогенную ситуацию в информационно-коммуникационной сфере;

совершенствование сил государственной системы, в том числе на основе внедрения современных информационно-коммуникационных технологий, информационно-аналитического обеспечения деятельности по противодействию противоправным деяниям;

разработку и внедрение в деятельность государственных органов, органов государственной власти субъектов Российской Федерации и организаций, участвующих в противодействии противоправным деяниям, информационных банков (баз) данных, информационно-телекоммуникационных сетей, автоматизированных систем и аппаратно-программных комплексов с применением передовых информационных технологий;

своевременную подготовку предложений по созданию и совершенствованию нормативно-правовой базы информационно-аналитического обеспечения противодействия противоправным деяниям;

систематическое повышение профессиональной подготовки специалистов в области противодействия противоправным деяниям.

Приоритетными направлениями научно-технических разработок в области противодействия противоправным деяниям должны стать создание и внедрение новых программных продуктов для совершенствования деятельности сил государственной системы, способных существенно повысить эффективность борьбы с преступлениями и правонарушениями, совершаемыми с использованием информационно-коммуникационных технологий, и сократить время на проведение оперативных мероприятий.

Информационно-аналитическое обеспечение создания и функционирования государственной системы включает в себя сбор, хранение, систематизацию, анализ, оценку информации о правонарушениях и преступлениях, совершаемых с использованием информационно-коммуникационных технологий, а также обмен такой информацией с заинтересованными органами и организациями.

Информационно-аналитическое обеспечение может включать создание и разработку единого методического подхода (криминалистической методики) расследования преступлений, связанных с использованием информационно-коммуникационных технологий, который позволит аккумулировать отечественный и иностранный положительный опыт в указанном направлении в целях повышения эффективности расследования уголовных дел данной категории преступлений.

К деятельности по информационно-аналитическому обеспечению создания и функционирования государственной системы привлекаются научно-исследовательские организации, а также общественные объединения и другие институты гражданского общества.

Продуманная кадровая политика является одним из основных направлений успешного создания и функционирования государственной системы. Подразделения, участвующие в противодействии противоправным деяниям, должны быть укомплектованы высококвалифицированными специалистами, обладающими необходимыми качествами и навыками. Приоритетным направлением кадровой политики является повышение престижа службы в указанных подразделениях.

Кадровое обеспечение создания и функционирования государственной системы осуществляется по следующим основным направлениям:

систематическое повышение квалификации, подготовка и переподготовка сотрудников, участвующих в противодействии преступлениям, совершаемым с использованием информационно-коммуникационных технологий;

специализация сотрудников подразделений безопасности негосударственных организаций с учетом специфики решаемых ими задач;

создание экспертно-консультативных групп из числа сотрудников, обладающих специальными знаниями и навыками.

Организационно-штатное обеспечение создания и функционирования государственной системы осуществляется за счет имеющейся штатной численности заинтересованных государственных органов и соответствующих институтов гражданского общества.

Финансовое обеспечение создания и функционирования государственной системы осуществляется за счет средств федерального бюджета, бюджетов субъектов Российской Федерации, местных бюджетов и средств хозяйствующих субъектов.

V. Основные направления совершенствования деятельности по выявлению, раскрытию, пресечению и предупреждению правонарушений и преступлений, совершаемых с использованием информационно-коммуникационных технологий и ожидаемые результаты реализации настоящей Концепции

Принимая во внимание специфику рассматриваемых противоправных деяний, наиболее эффективным способом их пресечения и выявления можно считать выработку модели взаимодействия правоохранительных, финансовых и иных государственных органов, а также привлечение к сотрудничеству организаций и институтов гражданского общества.

Основными направлениями совершенствования деятельности по выявлению, раскрытию, пресечению и предупреждению правонарушений и преступлений, совершаемых с использованием информационно-коммуникационных технологий, являются:

организация и проведение мероприятий, направленных на профилактику противоправных деяний; совершенствование законодательства в сфере противодействия противоправным деяниям; выработка дополнительного инструментария, направленного на возмещение причиненного ущерба.

Ожидаемыми результатами реализации настоящей Концепции являются:

снижение темпов прироста преступлений и правонарушений, совершаемых с использованием информационно-коммуникационных технологий, и увеличение доли возмещенного материального ущерба, причиненного потерпевшим;

совершенствование взаимодействия государственных органов, реализующих настоящую Концепцию;

повышение уровня раскрываемости преступлений, совершенных с использованием информационно-коммуникационных технологий;

активное участие институтов гражданского общества в профилактике и предупреждении преступлений и правонарушений, совершаемых с использованием информационно-коммуникационных технологий;

повышение уровня правовой, финансовой и цифровой грамотности граждан в информационно-коммуникационной сфере;

развитие эффективного международного сотрудничества в сфере противодействия противоправным деяниям.

VI. Механизмы координации и организации межведомственного взаимодействия государственных органов, организаций и институтов гражданского общества по вопросам противодействия правонарушениям и преступлениям, совершаемым с использованием информационно-коммуникационных технологий

Реализацию настоящей Концепции осуществляют федеральные органы исполнительной власти, иные государственные органы, органы государственной власти субъектов Российской Федерации и органы местного самоуправления в соответствии с их компетенцией.

Обеспечение согласованных действий федеральных государственных органов, органов государственной власти субъектов Российской Федерации, Центрального банка Российской Федерации, финансовых и иных организаций при реализации мер в области противодействия противоправным деяниям осуществляется на площадке сформированных межведомственных комиссий, реализующих в том числе функции, направленные на обеспечение общественной безопасности и борьбу с преступностью, предупреждение преступлений и правонарушений, развитие информационных технологий и расширение их использования.

Реализация настоящей Концепции осуществляется в соответствии с планом мероприятий, утверждаемым Правительством Российской Федерации.

Приложение 3

УТВЕРЖДЕН
распоряжением Правительства
Российской Федерации
от 14 августа 2025 г. № 2207-р

ПЛАН
мероприятий по реализации Концепции государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий

	Наименование мероприятия	Ответственный исполнитель (соисполнители)	Срок реализации	Результат выполнения мероприятия
	I. Совершенствование законодательства в сфере противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий			
1.	Определение объема обрабатываемых персональных данных, необходимых хозяйствующим субъектам для осуществления своей деятельности	Роскомнадзор (созыв), Минцифры России, МВД России, Минэкономразвития России, Минфин России, ФСБ России, Росфинмониторинг во взаимодействии с Генеральной прокуратурой Российской Федерации, Следственным комитетом Российской Федерации и Банком России	IV квартал 2026 г.	Представление в Правительство Российской Федерации предложений по определению объема обрабатываемых персональных данных, необходимых хозяйствующим субъектам для осуществления своей деятельности

	Наименование мероприятия	Ответственный исполнитель (соисполнители)	Срок реализации	Результат выполнения мероприятия
2.	Проработка вопроса об определении объема сведений о регистрации, авторизации (прекращении регистрации) пользователей и сроков их хранения для владельцев сайтов, страниц сайтов в информационно-телекоммуникационной сети «Интернет», информационных систем и (или) программ для электронно — вычислительных машин (далее соответственно — организаторы распространения информации, сеть «Интернет»)	МВД России (созыв), Минцифры России, Минэкономразвития России, ФСБ России во взаимодействии с Генеральной прокуратурой Российской Федерации, Следственным комитетом Российской Федерации и Банком России	III квартал 2027 г.	Определение объема сведений, хранимых организаторами распространения информации
3.	Проработка вопроса об установлении обязанности операторов связи, интернет-провайдеров, организаторов распространения информации, организаций, предоставляющих услуги хостинга, и провайдеров услуг в сфере виртуальных активов по уведомлению правоохранительных органов, осуществляющих оперативно-разыскную деятельность, о случаях выявления признаков преступлений и административных правонарушений, совершаемых с использованием информационно-коммуникационных технологий (далее — противоправные деяния)	МВД России (созыв), Минцифры России, ФСБ России, Роскомнадзор во взаимодействии с Генеральной прокуратурой Российской Федерации и Следственным комитетом Российской Федерации	III квартал 2027 г.	Представление в Правительство Российской Федерации предложений по внесению изменений в законодательство Российской Федерации, направленных на повышение эффективности деятельности правоохранительных органов по предотвращению и пресечению противоправных деяний

	Наименование мероприятия	Ответственный исполнитель (соисполнители)	Срок реализации	Результат выполнения мероприятия
4.	Увеличение сроков давности привлечения к административной ответственности за совершение противоправных деяний и повышение ответственности за нарушение законодательства Российской Федерации в области персональных данных	МВД России (созыв), Минцифры России, Минэкономразвития России, ФСБ России, Роскомнадзор во взаимодействии с Генеральной прокуратурой Российской Федерации и Следственным комитетом Российской Федерации	III квартал 2027 г.	Внесение изменений в законодательство Российской Федерации об административных правонарушениях в части повышения эффективности административного преследования лиц, совершивших противоправные деяния
5.	Совершенствование уголовного, уголовно-процессуального законодательства и законодательства об оперативно-разыскной деятельности в части повышения эффективности деятельности правоохранительных органов по выявлению, предупреждению, раскрытию и расследованию противоправных деяний и обеспечению защиты прав потерпевших	МВД России (созыв), Минцифры России, Минэкономразвития России, ФСБ России, Росфинмониторинг во взаимодействии с Генеральной прокуратурой Российской Федерации, Следственным комитетом Российской Федерации и Банком России	IV квартал 2027 г.	Повышение эффективности деятельности правоохранительных органов по выявлению, предупреждению, раскрытию и расследованию противоправных деяний и обеспечению защиты прав потерпевших
II. Совершенствование профилактики противоправных деяний				
6.	Реализация мер по вовлечению граждан в мероприятия, направленные на профилактику противоправных деяний, в том числе в мероприятия по противодействию распространению информации противоправного характера в сети «Интернет»	МВД России (созыв), Минцифры России, ФСБ России во взаимодействии с Генеральной прокуратурой Российской Федерации и Следственным комитетом Российской Федерации	Постоянно	Увеличение числа граждан, вовлеченных в мероприятия, направленные на профилактику противоправных деяний

	Наименование мероприятия	Ответственный исполнитель (соисполнители)	Срок реализации	Результат выполнения мероприятия
7.	Реализация мер, направленных на повышение уровня цифровой и финансовой грамотности граждан и их ответственного отношения к использованию информационно-коммуникационных технологий, культуры поведения в цифровом пространстве	Минцифры России (созыв), Минкультуры России, Минфин России, Минобрнауки России, Минпросвещения России, МВД России во взаимодействии с Банком России	Постоянно	Повышение уровня цифровой и финансовой грамотности граждан и их ответственного отношения к использованию информационно-коммуникационных технологий, культуры поведения в цифровом пространстве
8.	Реализация мер, направленных на повышение уровня осведомленности граждан, в первую очередь социально уязвимых слоев населения, о методах совершения противоправных деяний и способах защиты от них, в том числе посредством размещения социальной рекламы, направленной на воспитание у граждан цифровой грамотности	Минкультуры России (созыв), Минфин России, МВД России, Минцифры России, Минпросвещения России, Минобрнауки России, Минтруд России, Минэкономразвития России, ФСБ России, Роскомнадзор, Росмолодежь во взаимодействии с Генеральной прокуратурой Российской Федерации, Следственным комитетом Российской Федерации и Банком России	Постоянно	Снижение уровня виктимного поведения граждан
9.	Организация и проведение мероприятий по предупреждению вовлечения несовершеннолетних в противоправную деятельность в информационно-коммуникационной сфере	Росмолодежь (созыв), Минпросвещения России, Минобрнауки России, МВД России, Минфин России, Роскомнадзор во взаимодействии со Следственным комитетом Российской Федерации и Банком России	Постоянно	Снижение доли несовершеннолетних, вовлеченных в противоправную деятельность в информационно-коммуникационной сфере, повышение уровня их правовой, финансовой и цифровой грамотности в информационно-коммуникационной сфере

	Наименование мероприятия	Ответственный исполнитель (соисполнители)	Срок реализации	Результат выполнения мероприятия
10.	Совершенствование механизмов мониторинга соблюдения требований законодательства Российской Федерации о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, банковского законодательства, законодательства Российской Федерации в области связи, а также законодательства Российской Федерации о национальной платежной системе	Росфинмониторинг (созыв), Роскомнадзор, Минцифры России во взаимодействии с Генеральной прокуратурой Российской Федерации и Банком России	Постоянно	Представление в Правительство Российской Федерации предложений по повышению эффективности мониторинга соблюдения требований законодательства Российской Федерации о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, банковского законодательства, законодательства Российской Федерации в области связи, а также законодательства Российской Федерации о национальной платежной системе
	III. Организационные, технические и иные меры противодействия противоправным деяниям			
11.	Подготовка предложений по использованию механизма государственно-частного партнерства в целях противодействия противоправным деяниям	Минцифры России (созыв), МВД России, Минэкономразвития России, ФСБ России во взаимодействии с Генеральной прокуратурой Российской Федерации, Следственным комитетом Российской Федерации и Банком России	II квартал 2026 г.	Представление в Правительство Российской Федерации предложений по использованию механизма государственно-частного партнерства в целях противодействия противоправным деяниям

	Наименование мероприятия	Ответственный исполнитель (соисполнители)	Срок реализации	Результат выполнения мероприятия
12.	Создание депозитария профилактических материалов в сфере противодействия противоправным деяниям и поддержание его в актуальном состоянии для использования в профилактической деятельности	Минцифры России (созыв), МВД России, Минэкономразвития России, Роскомнадзор во взаимодействии с Генеральной прокуратурой Российской Федерации, Следственным комитетом Российской Федерации и Банком России	II квартал 2026 г., далее — постоянно	Распространение профилактических материалов в сфере противодействия противоправным деяниям
13.	Проработка вопроса о целесообразности создания единого реестра адресов электронных ссылок на официальные сайты хозяйствующих субъектов, на законных основаниях осуществляющих деятельность посредством сети «Интернет», в целях повышения эффективности ограничения доступа к подменным (фишинговым) ресурсам за счет их своевременного выявления методом исключения	Минцифры России (созыв), МВД России, Минфин России, ФНС России, Роскомнадзор во взаимодействии с Генеральной прокуратурой Российской Федерации и Банком России	III квартал 2026 г.	Представление в Правительство Российской Федерации предложений по созданию единого реестра адресов электронных ссылок на официальные сайты хозяйствующих субъектов, на законных основаниях осуществляющих деятельность посредством сети «Интернет»
14.	Проработка вопроса о повышении эффективности идентификации лиц при регистрации доменных имен, а также об упрощении процедуры прекращения регистрации доменных имен, используемых для фишинга и в иных противоправных целях	Минцифры России (созыв), МВД России, Роскомнадзор, Минфин России во взаимодействии с Генеральной прокуратурой Российской Федерации и Банком России	III квартал 2026 г.	Представление в Правительство Российской Федерации предложений о повышении эффективности идентификации лиц при регистрации доменных имен, а также об упрощении процедуры прекращения регистрации доменных имен, используемых для фишинга и в иных противоправных целях

	Наименование мероприятия	Ответственный исполнитель (соисполнители)	Срок реализации	Результат выполнения мероприятия
15.	Принятие мер по контролю за соблюдением законодательства Российской Федерации, в том числе налогового, лицами, осуществляющими деятельность в сфере обращения цифровых валют, проработка вопроса о совершенствовании порядка ведения реестра таких лиц	МВД России, Минэкономразвития России, ФНС России, ФСБ России во взаимодействии с Генеральной прокуратурой Российской Федерации и Банком России	IV квартал 2026 г.	Усиление контроля за обращением цифровых валют
16.	Разработка и реализация механизмов проверки абонентских номеров, используемых при аутентификации и авторизации пользователей в информационных системах государственных органов и организаций, оказывающих социально значимые цифровые услуги, на принадлежность пользователям и механизмов открепления таких абонентских номеров от учетных записей указанных пользователей в случае расторжения договоров об оказании услуг связи	Минцифры России (созыв), Минфин России, МВД России, Минэкономразвития России, Роскомнадзор, ФСБ России	IV квартал 2026 г.	Предотвращение доступа злоумышленников к информационным системам государственных органов и организаций, оказывающих социально значимые цифровые услуги, с использованием не принадлежащих им абонентских номеров
17.	Проработка вопроса о возможности интеграции в основные мобильные приложения, используемые для взаимодействия с органами государственной власти, а также в банковские и социально значимые мобильные приложения модуля обязательного информирования граждан о возможных противоправных деяниях	Минцифры России (созыв), МВД России во взаимодействии с Генеральной прокуратурой Российской Федерации и Банком России	I квартал 2027 г.	Повышение уровня защищенности граждан от противоправных деяний

	Наименование мероприятия	Ответственный исполнитель (соисполнители)	Срок реализации	Результат выполнения мероприятия
18.	Проработка вопроса о возможности введения механизма добровольного согласия граждан на ограничение доступа к потенциально опасной информации, распространяемой посредством информационно-телекоммуникационных сетей, включая сеть «Интернет», доступ к которой на территории Российской Федерации не ограничен	Минцифры России (созыв), Минкультуры России, Роскомнадзор, Росмолодежь, заинтересованные федеральные органы исполнительной власти	III квартал 2027 г.	Представление в Правительство Российской Федерации предложений по предоставлению гражданам возможности добровольного ограничения их доступа к потенциально опасной информации, распространяемой посредством информационно-телекоммуникационных сетей, включая сеть «Интернет»
19.	Проработка вопроса о наделении органов, осуществляющих оперативно-разыскную деятельность, возможностью ограничения оказания услуг в информационно-коммуникационной сфере в случаях возникновения непосредственной угрозы жизни и здоровью граждан, государственной, военной, экономической, информационной или экологической безопасности Российской Федерации	МВД России (созыв), Минцифры России, ФСБ России во взаимодействии с Генеральной прокуратурой Российской Федерации	IV квартал 2027 г.	Повышение эффективности деятельности органов, осуществляющих оперативно-разыскную деятельность, по предупреждению противоправных деяний
20.	Проработка вопроса о разработке алгоритма выявления технологий искусственного интеллекта в противоправной деятельности	Минцифры России, МВД России, Роскомнадзор	I квартал 2028 г.	Разработка технических мер выявления технологий искусственного интеллекта в противоправной деятельности

	Наименование мероприятия	Ответственный исполнитель (соисполнители)	Срок реализации	Результат выполнения мероприятия
21.	Проведение мероприятий в информационно-телекоммуникационных сетях, включая сеть «Интернет», направленных на повышение эффективности ограничения доступа к информации, распространение которой в Российской Федерации запрещено	Роскомнадзор (созыв), Минцифры России, ФСБ России, МВД России, Росмолодежь во взаимодействии с Генеральной прокуратурой Российской Федерации и Банком России	Постоянно	Реализация мероприятий по ограничению доступа граждан к информации, распространение которой в Российской Федерации запрещено
22.	Разработка и реализация мер, направленных на выявление специального телекоммуникационного оборудования, используемого при совершении противоправных деяний, и ограничение его оборота	МВД России (созыв), Минцифры России, Минпромторг России, Роскомнадзор, ФСБ России во взаимодействии с Генеральной прокуратурой Российской Федерации и Следственным комитетом Российской Федерации	Постоянно	Ограничение незаконного использования специального телекоммуникационного оборудования
23.	Применение технологий искусственного интеллекта, нейронных сетей и машинного обучения в деятельности по выявлению в сети «Интернет» информации, распространение которой в Российской Федерации запрещено, в целях последующего ограничения доступа к такой информации	Роскомнадзор (созыв), Минцифры России, МВД России, ФСБ России во взаимодействии с Генеральной прокуратурой Российской Федерации и Следственным комитетом Российской Федерации	Постоянно	Повышение эффективности выявления в сети «Интернет» информации, распространение которой в Российской Федерации запрещено
24.	Осуществление мониторинга сети «Интернет» в целях выявления новых видов потенциально опасной информации и принятие мер к ограничению ее распространения, в том числе путем отнесения к категории запрещенной	МВД России (созыв), Минцифры России, Минкультуры России, Минобрнауки России, Минэкономразвития России, Минобороны России, Роскомнадзор, ФСБ России, Рособрнадзор, Росмолодежь	Постоянно	Сокращение объема потенциально опасной информации, распространяемой в сети «Интернет»

	Наименование мероприятия	Ответственный исполнитель (соисполнители)	Срок реализации	Результат выполнения мероприятия
		во взаимодействии с Генеральной прокуратурой Российской Федерации и Следственным комитетом Российской Федерации		
IV. Кадровое обеспечение деятельности по противодействию противоправным деяниям				
25.	Разработка и реализация мер поддержки молодых специалистов, занятых в сфере противодействия противоправным деяниям, в том числе занимающихся производством судебных экспертиз в сфере информационно-коммуникационных технологий, содействие их профессиональному развитию. Проработка вопроса об отсрочке от призыва указанных специалистов на военную службу	МВД России, Минцифры России, Минобороны России, Минтруд России, Росмолодежь, Росфинмониторинг, заинтересованные федеральные органы исполнительной власти во взаимодействии со Следственным комитетом Российской Федерации	III квартал 2026 г., далее — постоянно	Комплектование государственных органов и организаций, осуществляющих деятельность в сфере противодействия противоправным деяниям, профильными специалистами
26.	Принятие дополнительных мер по систематическому повышению квалификации, подготовке и переподготовке сотрудников, участвующих в противодействии противоправным деяниям, подготовка квалифицированных специалистов в сфере информационной безопасности, экспертов в области информационно-коммуникационных технологий, оснащение их современным программным обеспечением, оборудованием и криминалистическими	МВД России, Минцифры России, ФСБ России, заинтересованные федеральные органы исполнительной власти во взаимодействии с Генеральной прокуратурой Российской Федерации, Следственным комитетом Российской Федерации и Банком России	Постоянно	Увеличение числа квалифицированных специалистов и экспертов, участвующих в противодействии противоправным деяниям

	Наименование мероприятия	Ответственный исполнитель (соисполнители)	Срок реализации	Результат выполнения мероприятия
	средствами, разработка и внедрение новых технологий для перехвата, сохранения и использования цифровых доказательств. Организация межведомственной стажировки (обмена опытом), в том числе по применению специализированных средств защиты от противоправных деяний			
V. Развитие международного сотрудничества в сфере противодействия противоправным деяниям				
27.	Подготовка к подписанию Конвенции Организации Объединенных Наций против киберпреступности; укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям (далее — Конвенция)	МИД России (созыв), Минюст России, МВД России, Минцифры России, ФСБ России, СВР России во взаимодействии с Генеральной прокуратурой Российской Федерации и Следственным комитетом Российской Федерации	IV квартал 2025 г.	Подписание Конвенции
28.	Разработка дополнительного протокола к Конвенции, соответствующего российским подходам к развитию международного сотрудничества в сфере противодействия киберпреступности, а также последующее его распространение по дипломатическим каналам	МИД России (созыв), Минюст России, МВД России, Минцифры России, ФСБ России, СВР России во взаимодействии с Генеральной прокуратурой Российской Федерации и Следственным комитетом Российской Федерации	IV квартал 2026 г.	Разработка дополнительного протокола к Конвенции

	Наименование мероприятия	Ответственный исполнитель (соисполнители)	Срок реализации	Результат выполнения мероприятия
29.	Организация работы по подготовке к ратификации Конвенции, в том числе формулирование заявлений и оговорок к ней, внесение соответствующих изменений в законодательство Российской Федерации	МИД России (созыв), Минюст России, МВД России, Минцифры России, ФСБ России, СВР России во взаимодействии с Генеральной прокуратурой Российской Федерации и Следственным комитетом Российской Федерации	IV квартал 2027 г.	Ратификация Конвенции
30.	Обеспечение сотрудничества с государствами – участниками Содружества Независимых Государств, государствами объединения БРИКС, государствами — членами Организации Договора о коллективной безопасности, Шанхайской организацией сотрудничества, Ассоциацией государств Юго-Восточной Азии, другими государствами и международными организациями по вопросам противодействия противоправным деяниям	МИД России (созыв), Минюст России, МВД России, Минцифры России, ФСБ России, СВР России, Росфинмониторинг во взаимодействии с Генеральной прокуратурой Российской Федерации, Следственным комитетом Российской Федерации и Банком России	Постоянно	Выстраивание эффективного межгосударственного взаимодействия в сфере противодействия противоправным деяниям
31.	Совершенствование обмена информацией между компетентными органами иностранных государств в рамках предупреждения, пресечения противоправных деяний и производства предварительного расследования по соответствующим уголовным делам	МВД России (созыв), Минюст России, ФСБ России, Росфинмониторинг во взаимодействии с Генеральной прокуратурой Российской Федерации и Следственным комитетом Российской Федерации	Постоянно	Выстраивание эффективного международного сотрудничества по противодействию противоправным деяниям с учетом необходимости преодоления двойных стандартов в подходах зарубежных

	Наименование мероприятия	Ответственный исполнитель (соисполнители)	Срок реализации	Результат выполнения мероприятия
				партнеров к уголовному преследованию лиц, совершивших противоправные деяния, а также адекватного использования имеющихся международных правовых инструментов
32.	Изучение и анализ международного опыта противодействия использованию в преступных целях информационно-коммуникационных технологий в целях подготовки государственными органами предложений по совершенствованию мер борьбы с противоправными деяниями	МВД России (созыв), МИД России, Минюст России, Минцифры России, Минэкономразвития России, ФСБ России, СВР России, Росфинмониторинг во взаимодействии с Генеральной прокуратурой Российской Федерации, Следственным комитетом Российской Федерации и Банком России	Постоянно	Совершенствование мер борьбы с противоправными деяниями
	VI. Развитие научного обеспечения в сфере противодействия противоправным деяниям			
33.	Проведение научных исследований, направленных на противодействие противоправным деяниям, в том числе связанных с изучением возможностей искусственного интеллекта	МВД России (созыв), Минцифры России, Минэкономразвития России, ФСБ России во взаимодействии с Генеральной прокуратурой Российской Федерации, Следственным комитетом Российской Федерации и Банком России	Постоянно	Выработка научно обоснованных подходов к выявлению и пресечению противоправных деяний

	Наименование мероприятия	Ответственный исполнитель (соисполнители)	Срок реализации	Результат выполнения мероприятия
34.	Реализация мер, направленных на прогнозирование угроз, связанных с противоправным использованием информационно-коммуникационных технологий, включая использование технологий искусственного интеллекта	МВД России, Минцифры России, ФСБ России, заинтересованные федеральные органы исполнительной власти во взаимодействии с Генеральной прокуратурой Российской Федерации, Следственным комитетом Российской Федерации и Банком России	Постоянно	Определение возможных сценариев развития угроз, связанных с противоправным использованием информационно-коммуникационных технологий, и выработка своевременных мер реагирования
35.	Проведение научно-исследовательских и опытно-конструкторских работ по разработке и применению криминалистических средств и методов предотвращения, пресечения, выявления, раскрытия и расследования противоправных деяний, а также сбора доказательств по ним	МВД России (созыв), Минцифры России, ФСБ России во взаимодействии с Генеральной прокуратурой Российской Федерации, Следственным комитетом Российской Федерации и Банком России	Постоянно	Разработка и внедрение новых криминалистических средств и методов противодействия противоправным деяниям
36.	Организация и проведение научно-практических мероприятий (конференций, семинаров, круглых столов, научных секций), посвященных противодействию противоправным деяниям	МВД России, Минцифры России, ФСБ России, Росфинмониторинг во взаимодействии с Генеральной прокуратурой Российской Федерации, Следственным комитетом Российской Федерации и Банком России	Постоянно	Обмен знаниями и опытом по разработке и внедрению новых криминалистических средств и методов предотвращения, пресечения, выявления, раскрытия и расследования противоправных деяний

	Наименование мероприятия	Ответственный исполнитель (соисполнители)	Срок реализации	Результат выполнения мероприятия
37.	Организация и обеспечение на постоянной основе деятельности экспертно-консультативной группы из числа представителей федеральных органов государственной власти, операторов связи, кредитно-финансовых учреждений, организаторов распространения информации по выявлению проблемных вопросов в деятельности по противодействию противоправным деяниям и по выработке предложений по их решению, включая проработку вопроса о расширении компетенции ИТ-компаний по проведению компьютерных экспертиз	МВД России (созыв), Минцифры России, Минэкономразвития России, Минобороны России, ФСБ России, Роскомнадзор, Росфинмониторинг во взаимодействии с Генеральной прокуратурой Российской Федерации, Следственным комитетом Российской Федерации и Банком России	Постоянно	Обмен знаниями и опытом противодействия противоправным деяниям, мониторинг правоприменительной практики, выработка рекомендаций по совершенствованию указанной деятельности, своевременное выявление и решение проблемных вопросов

Овчинский Владимир Семенович

Криминология цифрового мира

Учебник

2-е издание, дополненное и переработанное

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

ООО «Научно-издательский центр ИНФРА-М»
127282, Москва, ул. Полярная, д. 31в, стр. 1
Тел.: (495) 280-15-96, 280-33-86. Факс: (495) 280-36-29
E-mail: books@infra-m.ru. Internet: www.infra-m.ru

Редактор *Г. В. Ганина*
Корректор *Е. Ю. Бадареу*
Разработка серии: *А. Л. Бондаренко*
Верстка: *Г. В. Струкова*

Подписано в печать 00.00.00
Формат 60×90/16. Бумага офсетная
Гарнитура «Таймс». Печать цифровая
Усл. печ. л. 21,75. Уч.-изд. л. 19,8
Тираж 100 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)