Федеральное государственное казенное образовательное
учреждение высшего образования
«Восточно-Сибирский институт
Министерства внутренних дел Российской Федерации»

Е. З. Сидорова, О. П. Грибунов

ОСОБЕННОСТИ КВАЛИФИКАЦИИ И ПРЕДУПРЕЖДЕНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ (ЦИФРОВЫХ) ТЕХНОЛОГИЙ

Учебное пособие

Иркутск
Восточно-Сибирский институт МВД России
2024

УДК 343
ББК 67.628
С34

Печатается по решению редакционно-издательского совета
Восточно-Сибирского института МВД России

Рецензенты:
заместитель начальника УОПР ГУ ООП МВД России Г. Ф. Тепанян;
кандидат юридических наук, доцент, начальник кафедры уголовного права
УНК по ПС в ОВД Волгоградской академии МВД России В. В. Намнясева.

Сидорова, Екатерина Закариевна.

С34 Особенности квалификации и предупреждения преступлений, совершаемых с использованием информационных (цифровых) технологий : учебное пособие / Е. З. Сидорова, О. П. Грибунов. – Иркутск : Восточно-Сибирский институт МВД России, 2024. – 128 с. – ISBN 978-5-9538-0110-2.

В учебном пособии раскрыты основные уголовно-правовые характеристики отдельных видов цифровых преступлений, а также положения о превенции цифровой преступности. Дано определение цифровых преступлений, представлена авторская классификация подобных уголовно наказуемых деяний, озвучена актуальная криминологическая характеристика цифровой преступности, в том числе освещены особенности личностей цифрового преступника, его жертвы, а также детерминационный комплекс цифровой преступности. Самостоятельные главы пособия освещают основные направления превенции цифровой преступности и международный опыт сотрудничества государств по предупреждению киберпреступлений.

Пособие предназначено для курсантов, слушателей, адъюнктов, а также научно-педагогического состава образовательных организаций МВД России.

УДК 343
ББК 67.628

ISBN 978-5-9538-0110-2

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Цифровые технологии окружают нас повсюду. В современный период развития общества и государства уже нельзя представить человека, который никогда не пользовался мобильным телефоном, не обращался за государственной услугой, оказываемой посредством сети Интернет, в том или ином формате не принимал участие в интернет-конференции, не общался с близкими людьми посредством видеосвязи. Все это и многое другое стало доступным благодаря развитию цифровых технологий.

С другой стороны, развитие цифровых технологий повлекло за собой неизбежное возникновение угроз и опасностей, связанных с использованием информационных средств и систем. Подобные угрозы носят различный характер, в том числе криминальный. И к сожалению, в настоящее время, несмотря на все предпринимаемые меры защиты, угрозы продолжают существовать и мешают стабильному развитию общества и государства.

Президент России В. В. Путин, выступая на расширенном заседании коллегии МВД России в феврале 2022 года, подчеркнул, что в настоящее время особенно актуальной является проблема «новых вызовов, связанных с проникновением криминала в сферу информационных технологий и телекоммуникаций», и в этой связи необходимо «действовать на опережение, включая обновление нормативной базы, укрепление технических возможностей МВД России, поскольку кибертехнологии развиваются стремительно, возникают новые риски, и нужно их предупреждать, не позволять преступникам паразитировать на технологическом прогрессе»[1].

В этой связи необходимой и целесообразной представляется выработка единой государственной стратегии, направленной на защиту цифрового пространства от различных угроз и криминальных вызовов. Разработка подобной стратегии невозможна без научных исследований, посвященных формам и методам борьбы с правонарушениями, совершаемыми с использованием информационных технологий. Данное положение обосновывает актуальность настоящего учебного пособия.

Целью пособия является раскрытие уголовно-правовых особенностей некоторых составов цифровых преступлений, а также исследование криминологически значимых характеристик современной цифровой преступности и разработка на данной основе ключевых мер, направленных на предупреждение преступлений, совершаемых в информационном пространстве.

---

[1] Расширенное заседание коллегии МВД // Официальное интернет-представительство Президента России : сайт. URL: http://www.kremlin.ru/events/president/transcripts/70744. Дата публикации: 20.03.2023.

Задачами пособия являются:

– уголовно-правовая характеристика преступлений, совершаемых с использованием информационных (цифровых) технологий;

– определение особенностей квалификации преступлений, совершаемых с использованием информационных (цифровых) технологий;

– анализ уголовной политики в сфере обеспечения цифровой безопасности;

– криминологический анализ преступности в сфере информационных (цифровых) технологий;

– выявление особенностей личностей преступника, совершающего преступления с использованием информационных (цифровых) технологий, и его жертвы;

– исследование основ предупреждения преступлений, совершаемых с использованием информационных (цифровых) технологий;

– анализ международного опыта сотрудничества государств по предупреждению преступлений, совершаемых с использованием информационных (цифровых) технологий.

Изучение уголовно-правовых и криминологических особенностей цифровой преступности является обоснованным и необходимым на современном этапе развития общества и государства. Современный мир в большей степени ориентирован на переход в цифровое пространство, и поскольку преступность активно использует в своих криминальных целях информационные (цифровые) технологии, правоприменитель, занимающийся борьбой с цифровыми преступлениями, нуждается в теоретически обоснованных исследованиях по данной тематике.

Учебное пособие предназначено для исследователей, преподавателей, специалистов, обучающихся образовательных организаций высшего образования, интересующихся вопросами уголовно-правового противодействия преступлениям, совершаемым с использованием информационных (цифровых) технологий.

ГЛАВА 1.
УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ (ЦИФРОВЫХ) ТЕХНОЛОГИЙ

§ 1. Понятие преступлений, совершаемых с использованием информационных (цифровых) технологий

Как известно, все составы преступлений предусмотрены в Уголовном кодексе Российской Федерации[2]. Иных нормативных правовых актов, обеспечивающих уголовно-правовую охрану общественных отношений, нет. Романо-германская правовая система, на которой строится современная российская правовая база, позволяет сформировать уголовный закон, группируя все составы преступлений в зависимости от охраняемого блага (объекта). Соответственно, Особенная часть УК РФ состоит из разделов, глав и статей. Однако, несмотря на то, что преступления, совершаемые с использованием информационных (цифровых) технологий, занимают значительное место в структуре современной преступности, самостоятельного раздела или главы, посвященных данным видам преступлений, в действующем уголовном законе нет. Исключение составляет только глава 28 «Преступления в сфере компьютерной информации», но преступления данной главы составляют только небольшую часть всей цифровой преступности (данный вопрос раскроем ниже).

В связи с этим считаем целесообразным на теоретическом уровне определить, какие именно виды преступлений следует относить к преступлениям, совершаемым с использованием информационных (цифровых) технологий. Для этого обратимся к дефиниции данного термина.

В научной литературе можно встретить различные термины, характеризующие цифровые преступления:

– преступления, совершаемые с использованием информационных технологий[3];

---

[2] Уголовный кодекс Российской Федерации : УК : принят Гос. Думой 24 мая 1996 года : одобрен Советом Федерации 5 июня 1996 года : послед. ред. // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 13.12.2022).

[3] Ульянов, М. В. Преступления, совершаемые с использованием информационных технологий: динамика и тенденции // Общество и право : науч. журн. 2020. № 2 (72). С. 32–36.

– компьютерная преступность[4];

– преступность в сфере информационно-коммуникационных технологий[5];

– преступность в социальных сетях[6];

– киберпреступления[7];

– посягательства на цифровую информацию[8];

– информационные преступления[9];

– преступления в сфере высоких технологий[10];

– цифровая преступность[11] и т. д.

Такое научное разнообразие в использовании терминов, связанных с цифровыми преступлениями, стало возможным благодаря отсутствию единого понятия и определения в действующем законодательстве. В этой связи исследователи предпринимают попытки обосновать тот или иной термин, отражающий криминальную ситуацию в информационной среде.

В частности, при определении обозначенного феномена можно использовать термин «информационная преступность», предлагая тем самым рассмотрение цифровых преступлений (или киберпреступлений) только в контексте информационной сферы, элементом которой она

---

[4] Евдокимов, К. Н. Структура и состояние компьютерной преступности в Российской Федерации // Юридическая наука и правоохранительная практика : науч. журн. 2016. № 1 (35). С. 86–94.

[5] Ульянов, М. В. Противодействие преступности в сфере информационно-коммуникационных технологий в условиях применения карантинных мер // Национальная безопасность / Nota bene : электр. журн. 2020. № 2. С. 52–61. URL: https://www.e-notabene.ru/nbmag/article_32651.html?ysclid=lru3jg2a5z408562524 (дата обращения: 26.01.2024).

[6] Прокопенко, А. Н., Старостенко, И. Н. Основные направления международного сотрудничества России в области противодействия преступности в социальных сетях // Проблемы правоохранительной деятельности : междунар. науч.-теорет. журн. 2018. № 4. С. 53–59.

[7] Иванова, Л. В. Виды киберпреступлений по российскому уголовному законодательству // Юридические исследования : науч. журн. 2019. № 1. С. 25–33.

[8] Нечаева, Е. В., Латыпова, Э. Ю., Гильманов, Э. М. Посягательства на цифровую информацию: современное состояние проблемы // Человек: преступление и наказание : науч. журн. 2019. Т. 27 (1–4). № 1. С. 80–86.

[9] Гребеньков, А. А. Понятие информационных преступлений, место в уголовном законодательстве России и место признаков информации в структуре их состава // Lex Russica (Русский закон) : науч. юрид. журн. 2018. № 4 (137). С. 108–120.

[10] Чечель, Г. И., Третьяк, М. И. Законодательная регламентация преступлений против собственности в сфере высоких технологий в УК Казахстана и России // Всероссийский криминологический журнал : науч. журн. 2017. Т. 11. № 1. С. 228–236.

[11] Поляков, И. В. Цифровая преступность: проблемы понятийного аппарата, систематизации и правоприменительной практики // Проблемы правоохранительной деятельности : междунар. науч.-теорет. журн. 2020. № 4. С. 21–25.

является. Между тем компьютерная информация является специфичным видом информации, а кроме того, формально представляет собой объект самостоятельной уголовно-правовой охраны, что не дает возможности ее рассмотрения в контексте информационной сферы – так же, как и компьютерные преступления не могут быть рассмотрены как информационные преступления.

Можно использовать понятие «компьютерная преступность», предполагая рассмотрение исследуемого феномена в качестве преступности, совершаемой с помощью ЭВМ, высоких технологий.

Вместе с тем мы придерживаемся позиции авторов, которые считают, что использование компьютера аналогично использованию любого инструмента или средства, применение которых возможно для того, чтобы совершенствовать то или иное преступление, а компьютерная сеть является средой или обстановкой совершения уголовно наказуемого деяния[12].

В связи с вышесказанным считаем возможным в нашем пособии использовать указанные термины как равнозначные, несмотря на то, что определенные отличия между ними все же есть. Если не вступать в научную дискуссию по данному вопросу, под преступлениями, совершаемыми с использованием информационных (цифровых) технологий, можно понимать уголовно наказуемые деяния, механизм совершения которых предполагает использование информационных (цифровых) технологий и (или) информационно-телекоммуникационных сетей. При этом подобные преступления могут угрожать информационной безопасности как прямо, так и косвенно.

Ключевым термином, на котором основывается раскрываемое нами понятие, является термин «информационные технологии». Согласно Федеральному закону от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[13] (далее – Федеральный закон № 149-ФЗ), информационные технологии – это процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

---

[12] Жмыхов, А. А. Компьютерная преступность за рубежом и ее предупреждение : дис. … канд. юрид. наук. М., 2003. С. 56.

[13] Об информации, информационных технологиях и о защите информации : Федер. закон № 149-ФЗ : принят Гос. Думой 8 июля 2006 года : одобрен Советом Федерации 14 июля 2006 года : послед. ред. // КонсультантПлюс : сайт. URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 21.06.2023).

Кроме того, следует определить, что понимается под цифровыми технологиями. Современное законодательство не дает определения указанного термина, однако активно его использует (например, в настоящее время действует Паспорт федерального проекта «Цифровые технологии»[14]).

В научной литературе также можно встретить различные определения раскрываемого термина. В частности, под цифровыми технологиями понимаются технологии, которые используют компьютеры и (или) другую современную технику для записи кодовых импульсов и сигналов в определенной последовательности и с определенной частотой[15].

Цифровые технологии строятся на кодировании информации, переводе ее в цифровое значение («цифровые технологии» – от слова «цифра», словесная информация трансформируется в цифровой показатель) и передаче данной закодированной информации другому носителю, способному воспринять (расшифровать) полученную информацию.

Поскольку цифровые технологии очень масштабны и разнообразны по своему содержанию, можно говорить о различных видах цифровых технологий:

1) искусственный интеллект, машинное обучение, глубокое обучение;
2) компьютерное зрение;
3) нейросети;
4) блокчейн и криптовалюты;
5) большие данные;
6) телемедицина;
7) виртуальная и дополненная реальность;
8) кибербезопасность;
9) интернет вещей.

Кроме того, можно вести речь о различных сферах применения цифровых технологий: бизнес, образование, медицина, ритейл, искусство и развлечения, производство, общественное питание и многое другое.

---

[14] Паспорт федерального проекта «Цифровые технологии» : утв. президиумом Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности (протокол от 28 мая 2019 г. № 9) // Гарант : сайт. URL: https://base.garant.ru/72302272/ (дата обращения: 21.06.2023).

[15] Машевская, О. В. Цифровые технологии как основа цифровой трансформации современного общества // Вестник Полесского государственного университета. Серия общественных и гуманитарных наук : науч. журн. 2020. № 1. С. 37–44.

Таким образом, преступление, совершаемое с использованием информационных (цифровых) технологий, или цифровое преступление, или киберпреступление – это преступление, связанное с незаконным вторжением или доступом в компьютерные программы или данные. В обществе, которое все больше полагается на компьютеры (гаджеты), опасность цифровых преступлений постоянно возрастает. Киберпреступления являются преступной деятельностью, которая предполагает использование информационных технологий для незаконного или несанкционированного доступа к компьютерной системе (в широком понимании слова «компьютер») с намерением повреждения, удаления или изменения имеющейся там информации. Кроме того, к цифровым преступлениям можно относить и те преступления, которые совершаются посредством использования современных компьютерных технологий и средств связи.

§ 2. Виды преступлений, совершаемых с использованием информационных (цифровых) технологий

Именно потому, что цифровые технологии проникли практически во все сферы жизни общества, цифровая преступность сегодня особенно активизировалась и выросла. Относительно недавно в отчетах МВД России о состоянии преступности в стране появился раздел о преступлениях, совершаемых с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации. Представленные данные свидетельствуют о масштабности и распространенности подобных преступлений. Если в 2019 году было выявлено около 300 тысяч таких преступлений, то в 2022 году их число составило свыше 500 тысяч (таблица 1)[16]. Около четверти всех регистрируемых преступлений совершается при помощи Интернета, компьютера и других современных гаджетов. При этом можно вести речь только о зарегистрированных цифровых преступлениях, в то время как уровень криминальной латентности по-прежнему высок.

[16] Состояние преступности за 2019–2022 гг. // Министерство внутренних дел Российской Федерации : офиц. сайт. URL: https://мвд.рф/reports (дата обращения: 13.12.2022).

Таблица 1

Количество выявленных преступлений, совершаемых с использованием информационно-телекоммуникационных технологий в России в 2019–2022 гг.

год	2019	2020	2021	2022
Общее количество выявленных преступлений	2 024 337	2 044 221	2 004 404	1 966 795
темп прироста, %	-	*+1,0*	*-1,9*	*-1,9*
Количество выявленных преступлений, совершаемых с использованием информационно-телекоммуникационных технологий	294 409	510 396	517 722	522 065
удельный вес в общем числе, %	*14,5*	*25,0*	*25,8*	*26,5*
темп прироста, %	-	*+73,4*	*+1,4*	*+0,8*

К сожалению, официальные статистические показатели, характеризующие цифровую преступность, свидетельствуют о неуклонном росте числа подобных преступлений. И в этой связи особенно актуальными являются научные исследования, посвященные способам борьбы с данным видом преступности, методам и формам ее профилактики и раскрывающие особенности преступлений, совершаемых с использованием информационных (цифровых) технологий.

В научной литературе можно встретить различные точки зрения относительно того, какие именно составы преступлений следует относить к категории преступлений, совершаемых с использованием информационных (цифровых) технологий. Нам представляется, что большинство преступлений может быть совершено с использованием или применением тех или иных цифровых технологий, в том числе расчетных (пластиковых) карт, компьютерной техники, программных средств, фиктивных электронных платежей, информационно-телекоммуникационной сети Интернет, средств мобильной связи и иных. МВД России в своих отчетах о состоянии преступности в стране обращает внимание на следующие составы цифровых преступлений:

1) кража (ст. 158 УК РФ);

2) мошенничество (ст. 159 УК РФ);

3) мошенничество с использованием электронных средств платежа (ст. 159.3 УК РФ);

4) мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ);

5) незаконные организация и проведение азартных игр (ст. 171.2 УК РФ);

6) публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма (ст. 205.2 УК РФ);

7) незаконные производство, сбыт или пересылка наркотических средств, психотропных веществ, а также незаконные сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества (ст. 228.1 УК РФ);

8) изготовление порнографических материалов (ст. ст. 242, 242.1, 242.2 УК РФ);

9) публичные призывы к осуществлению экстремистской деятельности (ст. 280 УК РФ);

10) неправомерный доступ к компьютерной информации (ст. 272 УК РФ);

11) создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ).

Разумеется, данным списком перечень цифровых преступлений не ограничивается. Например, согласно ч. 2 ст. 128.1 УК РФ, клевета может быть совершена с использованием информационно-телекоммуникационных сетей, включая сеть Интернет. С использованием сети Интернет может быть совершено понуждение к действиям сексуального характера (ч. 3 ст. 134 УК РФ). Иными словами, существует большое количество составов преступлений, которые могут совершаться при помощи цифровых технологий.

Однако в настоящем пособии мы уделим внимание анализу тех составов преступлений, для которых использование современных информационных технологий наиболее характерно:

1) мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ);

2) неправомерный доступ к компьютерной информации (ст. 272 УК РФ);

3) создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ);

4) нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ);

5) неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ);

6) преступления, совершаемые в сфере оборота цифровых активов (криптовалюты) (на примере ст. ст. 205.1, 290 УК РФ).

ГЛАВА 2.
ОСОБЕННОСТИ КВАЛИФИКАЦИИ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ (ЦИФРОВЫХ) ТЕХНОЛОГИЙ

§ 1. Уголовно-правовая характеристика мошенничества в сфере компьютерной информации (ст. 159.6 УК РФ)

Статья 159.6 «Мошенничество в сфере компьютерной информации» была введена в действующее уголовное законодательство в ноябре 2012 года[17]. Согласно современной редакции УК РФ, мошенничество в сфере компьютерной информации – это хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

Данное преступление относится к категории преступлений небольшой тяжести (санкция статьи не предусматривает лишение свободы).

Особенность данного преступления заключается в его отличии от основного (классического) состава мошенничества, поскольку диспозиция статьи сконструирована законодателем таким образом, что способ совершения данного преступления – обман или злоупотребление доверием – не является обязательным элементом объективной стороны данного вида мошенничества. По сути, речь идет о новой форме хищения – «киберхищении», которое обладает своими характерными особенностями.

Необходимо раскрыть все обязательные элементы данного состава преступления.

1. Объект мошенничества в сфере компьютерной информации.

Родовой объект рассматриваемого нами преступления – сфера экономики (раздел VIII УК РФ «Преступления в сфере экономики»), т. е. сфера общественных отношений, связанных с производством, распределением и использованием материальных благ.

Видовой объект – интересы собственности (глава 21 УК РФ «Преступления против собственности»), т. е. общественные отношения,

[17] О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации : Федер. закон № 207-ФЗ : принят Гос. Думой 23 ноября 2012 года : одобрен Советом Федерации 28 ноября 2012 года : послед. ред. // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_138322/ (дата обращения: 20.03.2023).

обеспечивающие возможность владеть, пользоваться и распоряжаться соответствующими материальными благами как собственнику имущества, так и его владельцу.

Говоря о непосредственном объекте данного преступления, следует отметить, что мошенничество в сфере компьютерной информации относится к категории двуобъектных преступлений. Основным непосредственным объектом выступают общественные отношения в сфере собственности (поскольку ключевая цель данного преступления – завладеть чужим имуществом), а дополнительным – те общественные отношения, которые связаны с оборотом и использованием компьютерной информации, компьютерной техники, информационно-телекоммуникационных сетей[18].

Данное преступление является предметным. В качестве предмета следует рассматривать похищаемое имущество (как правило, речь идет о наличных и безналичных денежных средствах). С классической точки зрения, под имуществом в хищениях всегда понимались вещи, т. е. то, что обладает признаком материальности. Однако с развитием общественных отношений, с масштабным внедрением в нашу жизнь электронных и цифровых новаций подход, в том числе в судебной и правоприменительной практике, к определению понятия «имущество» изменился. В настоящее время в качестве предмета хищений, в том числе мошенничества в сфере компьютерной информации, понимаются не только овеществленные, материальные предметы окружающего мира, но и иные виды имущества и имущественные права, в том числе безналичные денежные средства, цифровая валюта, например биткоин, и иное.

Кроме того, учитывая двуобъектность рассматриваемого состава преступления, к предмету мошенничества в сфере компьютерной информации следует относить саму компьютерную информацию. Определение данного термина дано в примечании 1 к ст. 272 УК РФ «Неправомерный доступ к компьютерной информации» (иными словами, диспозицию статьи 159.6 УК РФ следует признать ссылочной). Согласно действующей редакции указанного примечания, компьютерная информация – это сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. В научной литературе можно встретить большое количество дискуссий относительно того, следует ли признать предложенное

[18] Барчуков, В. К. Непосредственный объект мошенничества в сфере компьютерной информации // Пробелы в российском законодательстве : юрид. науч. журн. 2018. № 7. С. 156.

законодателем определение удачным[19]. В частности, в современный период существуют технологии, работа которых не основывается на электрических сигналах, однако которые также направлены на получение и передачу компьютерной информации.

Наиболее значимым является уяснение того, в каких устройствах может храниться компьютерная информация. К таким устройствам, согласно разъяснениям Пленума Верховного Суда Российской Федерации, следует относить стационарные компьютеры, планшеты, ноутбуки, а также мобильные телефоны, смартфоны, платежные терминалы и иное[20].

В диспозиции описываемой статьи используется также термин «информационно-телекоммуникационные сети». Определение названного термина можно встретить в п. 4 ст. 2 Федерального закона № 149-ФЗ, согласно которому информационно-телекоммуникационная сеть – это технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники (в данном случае можно вести речь о бланкетной диспозиции описываемой уголовно-правовой нормы).

2. Объективная сторона мошенничества в сфере компьютерной информации.

Деяние рассматриваемого состава преступления может заключаться в следующем:

1) хищение чужого имущества;

2) приобретение права на чужое имущество.

Под хищением нужно понимать совершенные с корыстной целью противоправные безвозмездное изъятие и (или) обращение чужого имущества в пользу виновного или других лиц, причинившие ущерб собственнику или иному владельцу этого имущества (примечание 1 к ст. 158 УК РФ).

В свою очередь, под мошенническим приобретением права на чужое имущество можно понимать совершенное с корыстной целью противоправное, безвозмездное обращение такого права в пользу виновного или других лиц, причинившее ущерб владельцу этого права[21].

---

[19] Ефремова, М. А. К вопросу о понятии компьютерной информации // Российская юстиция : науч.-практ. журн. 2012. № 7. С. 50–52.

[20] О судебной практике по делам о мошенничестве, присвоении и растрате : Постановление Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 : послед. ред. // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_283918/ (дата обращения: 20.03.2023).

[21] Кобылин, П. О. Совершение мошенничества путем хищения или приобретения права на чужое имущество: вопросы законодательной регламентации // Законность и правопорядок : науч.-практ. журн. 2020. № 4 (28). С. 65.

Совершаемое по ст. 159.6 УК РФ хищение реализуется в форме мошенничества, однако, как мы уже говорили, способ данного преступления специфичен. Он заключается не в обмане потерпевшего или злоупотреблении его доверием, как в традиционном мошенничестве, а в следующих альтернативах:

1) ввод компьютерной информации;

2) удаление компьютерной информации;

3) блокирование компьютерной информации;

4) модификация компьютерной информации;

5) иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации;

6) иное вмешательство в функционирование информационно-телекоммуникационных сетей.

3. Субъект мошенничества в сфере компьютерной информации.

Субъект рассматриваемого нами состава преступления общий – физическое вменяемое лицо, достигшее 16-летнего возраста. При этом в ч. 3 ст. 159.6 УК РФ предусмотрен специальный субъект – лицо, использующее свое служебное положение.

4. Субъективная сторона мошенничества в сфере компьютерной информации.

Сконструированный законодателем состав преступления позволяет однозначно заключить, что данное преступление совершается только с прямым умыслом. Кроме того, как и для иных форм хищения, для мошенничества в сфере компьютерной информации характерно наличие корыстной цели.

Обращая внимание на квалифицированные и особо квалифицированные виды мошенничества в сфере компьютерной информации, можно отметить, что законодатель отнес к их числу такие признаки, как совершение данного преступления группой лиц по предварительному сговору и организованной группой, с причинением значительного ущерба, в крупном и особо крупном размере, лицом с использованием своего служебного положения, с банковского счета, а равно в отношении электронных денежных средств.

Так, согласно примечанию к ст. 158 УК РФ, значительный ущерб гражданину определяется с учетом его имущественного положения, но не может составлять менее 5 000 рублей; крупный размер – сумма, превышающая 250 000 рублей, а особо крупный – сумма, превышающая 1 000 000 рублей.

Вопрос квалификации деяний по ст. 159.6 УК РФ является сложным и на практике вызывает большое количество трудностей. Ключевой вопрос заключается в разграничении со смежными составами преступлений,

такими как ст. 158 УК РФ «Кража», ст. 159.3 УК РФ «Мошенничество с использованием электронных средств платежа», ст. 272 УК РФ «Неправомерный доступ к компьютерной информации» и т. д.

В научной литературе представлено мнение, каким образом разграничивать названные составы преступлений[22].

1. Хищение совершается путем использования учетных данных собственника или иного владельца имущества, независимо от способа получения доступа к таким данным (тайно либо путем обмана воспользовался телефоном потерпевшего, подключенным к услуге «мобильный банк», авторизовался в системе интернет-платежей под известными ему данными другого лица и т. п.). Такие действия, как кража, подлежат квалификации, если виновным не было оказано незаконное воздействие на программное обеспечение серверов, компьютеров или на сами информационно-телекоммуникационные сети (ст. 158 УК РФ).

2. Виновный, зная коды доступа, расплачивается в магазине, предъявляя кассиру принадлежащий потерпевшему мобильный телефон, на котором установлено приложение «Клиент-Банк» и есть функция бесконтактной оплаты. Он совершает мошенничество (путем обмана) с использованием электронных средств платежа (ст. 159.3 УК РФ).

3. Виновный, воздействуя на программное обеспечение серверов, компьютеров или сами информационно-телекоммуникационные сети, модифицирует компьютерную информацию, что позволяет совершить хищение чужого имущества (ст. 159.6 УК РФ). При этом требуется дополнительная квалификация его деяния по соответствующей части ст. 272 УК РФ либо (при наличии оснований) по ст. 273 УК РФ.

Однако это только одно из мнений по вопросу разграничения названных составов преступлений. В правоприменительной деятельности и научной литературе можно встретить иные подходы относительно данного сложного вопроса[23].

---

[22] Уголовное право Российской Федерации. Особенная часть : учебник / под ред. проф. М. В. Бавсуна; 2-е изд., перераб. и доп. Омск : Омская академия МВД России, 2020. С. 242.

[23] Густова, Э. В., Куликова, М. А. Уголовная ответственность за мошенничество с использованием электронных средств платежа (ст. 159.3 УК РФ) // Вестник экономической безопасности : науч. журн. 2021. № 4. С. 116.

§ 2. Уголовно-правовая характеристика неправомерного доступа к компьютерной информации (ст. 272 УК РФ) и создания, использования и распространения вредоносных компьютерных программ (ст. 273 УК РФ)

Статья 272 УК РФ посвящена уголовно-правовой защите от неправомерного доступа к компьютерной информации. В указанной статье речь идет об ответственности за неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации.

Специалисты отмечают, что не случайно глава «Преступления в сфере компьютерной информации» начинается именно с неправомерного доступа к компьютерной информации, поскольку данный состав олицетворяет собой универсальный информационный способ посягательства и представляет самое распространенное компьютерное преступление[24].

Обратим внимание, что отдельные вопросы квалификации преступлений по ст. 272 раскрываются в Постановлении Пленума Верховного Суда Российской Федерации от 15 декабря 2022 года № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть "Интернет"»[25]. Вместе с тем в связи с тем, что использование современных цифровых технологий стало повсеместным и масштабным, в одном документе все возникающие на практике вопросы, связанные с преступной деятельностью в сети Интернет, рассмотреть, конечно, было невозможно, поэтому можно признать, что названное нами Постановление Пленума Верховного Суда Российской Федерации носит рамочный характер.

Объект неправомерного доступа к компьютерной информации.

Непосредственным объектом преступления, предусмотренного ст. 272 УК РФ, является установленный собственником (владельцем) информационной системы режим обращения компьютерной информации.

---

[24] Уголовное право Российской Федерации. Особенная часть : учебник / под ред. проф. М. В. Бавсуна. С. 531.

[25] О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» : Постановление Пленума Верховного Суда Российской Федерации от 15 декабря 2022 года № 37 // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_434573/ (дата обращения: 21.06.2023).

Непосредственно режим реализуется через технические ограничения правомочий пользователей информационной системы в соответствии с правами доступа. Сущность неправомерного доступа заключается в обходе действия программно-технического модуля информационной системы, регламентирующего доступ к правомочиям, не соответствующим уровню делегирования собственника (владельца) информационной системы.

Предмет в данном составе преступлений представлен несколько нестандартным образом, что следует из толкования диспозиции «неправомерный доступ к охраняемой законом компьютерной информации». Большинство комментариев называют в качестве предмета преступления компьютерную информацию. Отдельные авторы считают, что подобный тезис является верным лишь отчасти, и объясняют это следующим: при таком ограничительном подходе компьютерная информация выступает некой «беспредметной субстанцией», которая существует сама по себе. Подобное представление о предмете данного преступления влечет неправильную установку для правоприменителей, отрывает от необходимой предметности в компьютерной сфере. Согласно теории уголовного права, предмет преступления отождествляется с предметом материального мира, воздействуя на который, субъект причиняет вред объекту преступления. Следовательно, компьютерная информация является лишь свойством предмета преступления, представленным в том числе информационным носителем в широком понимании. В любом случае, любые действия с компьютерной информацией влекут за собой ее изменение и вследствие этого находят отражение на каком-либо информационном носителе, позволяющем эти изменения зафиксировать[26].

Можно сказать, что предметом преступления, предусмотренного ст. 272 УК РФ, выступает не только информация сама по себе, но и информационный носитель, являющийся частью информационной системы, содержащий охраняемую законом компьютерную информацию. Перенос законодателем акцента исключительно на компьютерную информацию (свойство предмета) произведен для того, чтобы не перечислять всевозможные технические способы хранения информации, поскольку развитие компьютерных технологий происходит бурными темпами и виды носителей компьютерной информации находятся в постоянной, непрекращающейся модернизации. В этом смысле информационный носитель как предмет позволяет объединить материальную и информационную составляющие предмета преступления в конкретном предмете материального мира.

[26] Уголовное право Российской Федерации. Особенная часть : учебник / под ред. проф. М. В. Бавсуна. С. 532.

Под охраняемой законом информацией следует понимать такую информацию в рамках различных видов тайны, интеллектуальной собственности или части информационной системы, где собственники (владельцы) информации ограничивают доступ третьих лиц (при этом ресурсы Интернета террористического и экстремистского характера, а также содержащие призывы к насилию, порнографию, не подпадают под определение охраняемых законом, и, следовательно, их неправомерный взлом не может квалифицироваться по ст. 272 УК РФ).

Объективная сторона неправомерного доступа к компьютерной информации.

С внешней стороны данное преступление выражается в следующих необходимых признаках:

1) реализация активных действий в виде неправомерного доступа к компьютерной информации;

2) наступление преступных последствий в виде уничтожения, блокирования, модификации либо копирования компьютерной информации;

3) наличие причинной связи между действиями и наступившими последствиями.

Неправомерным доступ будет тогда, когда субъект не имеет законного основания для использования информационных ресурсов или владения ими, а также в тех случаях, когда лицо осуществляет доступ вопреки установленному владельцем информации или законом порядку.

Для определения сложносоставного понятия «неправомерный доступ» необходимо уяснить, что вообще следует понимать под доступом в содержательном и техническом плане, а также выделить критерии, позволяющие определить его неправомерный характер. Традиционно в любой информационной системе возможно выделить как минимум два уровня прав доступа:

1) модератор – это лицо, осуществляющее руководство проектом;

2) пользователь – это лицо, осуществляющее потребление услуг, предоставляемых информационной системой.

Таким образом, неправомерность доступа может выразиться в двух видах:

1) получение прав пользователя без разрешения собственника (самовольное получение прав доступа);

2) получение прав модератора лицом, имеющим статус пользователя системы, без разрешения собственника (самовольное расширение прав доступа).

Основным критерием определения неправомерности доступа является воля собственника. Она должна найти реальное выражение в установлении условий доступа и ограничений в форме преграды (системы

безопасности), позволяющей разделить всех лиц на «имеющих доступ» и «не обладающих данным доступом».

Таким образом, доступ к информации – это совершение конкретным лицом определенных действий с информацией, санкционированное владельцем или собственником.

Физическое завладение компьютером или носителем информации как имуществом не может квалифицироваться как неправомерный доступ к компьютерной информации и влечет ответственность за преступление против собственности или самоуправство. Не образует состава неправомерного доступа также уничтожение данных или носителя путем механического воздействия или посредством электромагнитного излучения. Подобные действия могут быть квалифицированы как умышленное уничтожение или повреждение имущества.

Законодатель связывает возникновение уголовной ответственности по ст. 272 УК РФ лишь с наступлением нематериальных последствий: уничтожением, блокированием, модификацией либо копированием информации.

Согласно названному нами ранее Постановлению Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37:

– уничтожение компьютерной информации – это приведение такой информации полностью или в части в непригодное для использования состояние с целью утраты возможности ее восстановления, независимо от того, имеется ли фактически такая возможность и была ли эта информация впоследствии восстановлена;

– блокирование компьютерной информации – это воздействие на саму информацию, средства доступа к ней или источник ее хранения, в результате которого становится невозможным в течение определенного времени или постоянно надлежащее ее использование, осуществление операций над информацией полностью или в требуемом режиме (искусственное затруднение или ограничение доступа законных пользователей к компьютерной информации, не связанное с ее уничтожением);

– модификация компьютерной информации – это внесение в нее любых изменений, включая изменение ее свойств, например целостности или достоверности;

– копирование компьютерной информации – это перенос имеющейся информации на другой электронный носитель при сохранении неизменной первоначальной информации либо ее воспроизведение в материальной форме (в том числе отправка по электронной почте, распечатывание на принтере, фотографирование, переписывание от руки и т. п.).

Важным элементом объективной стороны является установление причинной связи между неправомерным доступом и наступившими

последствиями. В технической сфере возможны ситуации причинения вреда в результате неисправностей или ошибок при функционировании средств вычислительной техники, что исключает ответственность за неправомерный доступ.

Часто неправомерному доступу предшествуют (сопутствуют) действия по применению вредоносных и шпионских программ, которые позволяют получить не только реквизиты доступа, но и значительные объемы конфиденциальной информации, что дает основания для дополнительной их квалификации по ст. 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ».

Раскрываемый нами состав материальный. Моментом окончания неправомерного доступа к компьютерной информации является наступление общественно опасных последствий, а именно уничтожение, блокирование, модификация, копирование компьютерной информации.

Субъект неправомерного доступа к компьютерной информации.

Субъект преступления, предусмотренного ч. ч. 1, 2 ст. 272 УК РФ, общий – это вменяемое физическое лицо, достигшее возраста 16 лет, а в ч. ч. 3, 4 ст. 272 УК РФ – как общий, так и специальный – лицо, использующее свое служебное положение.

Под лицом, использующим свое служебное положение, понимается лицо, получающее доступ к компьютеру в результате выполняемой работы или влияния по службе на лиц, имеющих такой доступ, т. е. тех, кто на законных основаниях использует компьютер, работает на нем или непосредственно обслуживает его работу (программисты, сотрудники, вводящие информацию в память компьютера, другие пользователи, а также системные администраторы локальных сетей, баз данных, специалисты по эксплуатации электронно-вычислительной техники и т. д.). Под доступом к компьютеру или сети следует понимать фактическую возможность использования компьютера при отсутствии права на работу с защищенной информацией. Программисты, системные администраторы, наладчики оборудования, технический персонал, обслуживающие компьютеры и сети, а также пользователи сети, являясь законными пользователями компьютерной системы, выходят за рамки своих функциональных обязанностей, получая доступ, которым они не наделены собственником или владельцем.

Субъективная сторона неправомерного доступа к компьютерной информации.

Субъективная сторона преступления, предусмотренного ст. 272 УК РФ, характеризуется прямым или косвенным умыслом.

Теперь обратим внимание на некоторые особенности квалифицированных видов неправомерного доступа к компьютерной информации.

В ч. 2 ст. 272 УК РФ речь идет о случаях неправомерного доступа к компьютерной информации, причинившего крупный ущерб или совершенного из корыстной заинтересованности.

Корыстная заинтересованность предполагает стремление лица путем неправомерного доступа к компьютерной информации или создания, использования или распространения вредоносной программы получить для себя или других лиц выгоду имущественного характера, не связанную с незаконным безвозмездным обращением имущества в свою пользу или в пользу других лиц. При этом возможно как получение какой-либо выгоды, так и освобождение от имущественных затрат (например, незаконное получение преимуществ в системе регистрации на сайте при покупке товара или услуги, получение скидок на сайте, освобождение от каких-либо имущественных затрат, оплаты услуг и т. д.).

В свою очередь, согласно примечанию к ст. 272 УК РФ, крупным признается ущерб, сумма которого превышает 1 000 000 рублей.

Интересно обратить внимание на ч. 4 ст. 272 УК РФ, согласно которой лицо привлекается к уголовной ответственности в случае неправомерного доступа к компьютерной информации, если это повлекло за собой тяжкие последствия или создало угрозу их наступления.

Тяжкие последствия – это категория, которая законодательно не определена, является оценочной, т. е. требует установления правоприменителем в каждом конкретном случае. Данный признак характеризуется как умышленной, так и неосторожной формами вины.

Тяжкие последствия могут быть сгруппированы по следующим категориям:

– физический вред (смерть одного или нескольких человек, причинение тяжкого вреда здоровью);

– имущественный ущерб (особо крупный материальный ущерб, упущенная выгода, катастрофы или аварии, существенный экологический ущерб);

– организационные последствия (нарушение безопасности государства, дезорганизация деятельности государственного органа или коммерческой организации, паника на рынке ценных бумаг или в банковской сфере).

Важно отметить, что состав преступления, предусмотренного ч. 4 ст. 272 УК РФ, является формально-материальным. Оно может быть окончено как в момент наступления тяжких последствий (и в этом случае данный состав является материальным), так и в момент создания хотя бы угрозы наступления тяжких последствий (и в этом случае состав формальный). Однако правоприменитель должен доказать, что такая угроза была реальной.

Теперь акцентируем внимание на уголовно-правовой характеристике ст. 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ».

Статья 273 УК РФ предусматривает ответственность за создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации.

Объект создания, использования и распространения вредоносных компьютерных программ.

Непосредственным объектом данного преступления являются общественные отношения, обеспечивающие безопасность компьютерной информации, компьютерной инфраструктуры и сетей.

В диспозиции ст. 273 УК РФ выделяются два типа компьютерной информации:

1) компьютерные программы, заведомо предназначенные для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации;

2) иная компьютерная информация, заведомо предназначенная для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации.

Под вредоносной программой следует понимать программы, специально созданные для совершения действий, не санкционированных собственником компьютера, которые могут приводить к нарушению нормального функционирования компьютерных программ. Наиболее распространенными видами вредоносных компьютерных программ являются «Червь», «Троян», «Spyware», «Adware», «Keylogger», «Ботнет», «Руткит», «Баннеры-вымогатели».

Для определения вредоносности программы следует использовать три критерия:

1. Функционирование программы приводит к самовольному уничтожению, блокированию, модификации либо копированию информации или нейтрализации средств защиты компьютерной информации, нарушению работы компьютера или компьютерной сети.

2. Операции, выполняемые программой, не санкционированы пользователем компьютера, т. е. происходят без ведома пользователя на системном уровне или обманывают пользователя, выдавая одну операцию за другую. Так, программа форматирования диска, входящая в комплект

любой операционной системы, не является по этому критерию вредоносной, так как ее запуск происходит по воле пользователя.

3. Заведомость означает, что программа создавалась с прямым умыслом, направленным на несанкционированное причинение вреда пользователю от результатов ее работы. Этот критерий позволяет отграничить программы, которые поставляются по различным типам лицензий и могут содержать ошибки, при определенных условиях причиняющие неосторожный вред.

Согласно названному нами ранее Постановлению Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37, к иной компьютерной информации могут быть отнесены любые сведения, которые, не являясь в совокупности компьютерной программой, позволяют обеспечить достижение целей, перечисленных в ч. 1 ст. 273 УК РФ (например, ключи доступа, позволяющие нейтрализовать защиту компьютерной информации, элементы кодов компьютерных программ, способных скрытно уничтожать и копировать информацию). В научной литературе отмечается, что к иной компьютерной информации могут быть отнесены требующие компиляции текстовые файлы с исходниками программ для взлома различных служб и программ операционной системы, интернет-сервисов и сайтов, библиотеки для создания вирусов, наборы данных для взлома системы через использование эксплойтов и т. д. К иной компьютерной информации, заведомо предназначенной для нейтрализации средств защиты компьютерной информации, относятся файлы различных типов, описывающие алгоритмы взлома лицензионного программного обеспечения, баз данных, средств защиты информации, установленных пользователем, и т. д.

Также отметим, что в Постановлении Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37 указывается, что под нейтрализацией средств защиты компьютерной информации следует понимать воздействие, в частности на технические, криптографические и другие средства, предназначенные для защиты компьютерной информации от несанкционированного доступа к ней, а также воздействие на средства контроля эффективности защиты информации (технические средства и программы, предназначенные для проверки средств защиты компьютерной информации, например осуществляющие мониторинг работы антивирусных программ) с целью утраты ими функций по защите компьютерной информации или контролю эффективности такой защиты.

Объективная сторона создания, использования и распространения вредоносных компьютерных программ.

Объективная сторона преступления характеризуется совершением любого из трех альтернативных действий:

1) создание вредоносных компьютерных программ (вредоносной компьютерной информации) – это деятельность, направленная на разработку, подготовку программ (в том числе путем внесения изменений в существующие программы) или иной компьютерной информации, предназначенных для несанкционированного доступа, т. е. совершаемого без согласия обладателя информации лицом, не наделенным необходимыми для такого доступа полномочиями, либо в нарушение установленного нормативными правовыми актами порядка уничтожения, блокирования, модифицирования, копирования компьютерной информации или нейтрализации средств ее защиты;

2) распространение вредоносных компьютерных программ (вредоносной компьютерной информации) – это предоставление доступа к ним конкретным лицам или неопределенному кругу лиц любым способом, включая продажу, рассылку, передачу копии на электронном носителе либо с использованием сети Интернет, размещение на серверах, предназначенных для удаленного обмена файлами;

3) использование вредоносных компьютерных программ (вредоносной компьютерной информации) – это действия, состоящие в их применении, в результате которого происходит умышленное уничтожение, блокирование, модификация, копирование компьютерной информации или нейтрализация средств ее защиты.

Вредоносная программа должна быть в форме компьютерного файла, воспринимаемого операционной системой как совокупность команд. Не следует признавать созданием вредоносной программы сохранение алгоритма или текста на языке программирования вредоносной программы в текстовом файле (за исключением командных файлов, имеющих расширение *.bat, *.cmd).

Использование вредоносной программы начинается с выполнения программного кода, который приводит к активации ее вредных свойств. Как правило, для вирусов это заражение (копирование и запуск вредоносной программы) компьютера, компьютерного носителя или компьютерной сети. Копирование компьютерного вируса в архиве, где невозможен его запуск, при определенных условиях может быть признано распространением.

Распространение вредоносной программы может быть совершено либо скрытно от пользователя, либо открыто – как размещение на сайте архива с вредоносной программой и инструкцией по применению для скачивания, как передача третьим лицам путем продажи, проката, сдачи внаем, предоставления взаймы. К распространению следует относить случаи встраивания в сайт под видом картинок или других файлов вредоносных программ, не обладающих свойствами по самораспространению (для программ «троянский конь»), рассылки по

почте или через sms, а также другие действия, в результате которых вредоносная программа оказывается скопированной на компьютер, цифровое устройство или информационный носитель третьих лиц, если она не запущена.

С объективной стороны, состав преступления, предусмотренный ч. 1 ст. 273 УК РФ, сконструирован как формальный, момент окончания зависит от совершаемых лицом действий: с момента появления программы, способной причинить вред компьютерной информации (для создания вредоносной программы и внесения изменений в существующие программы); с момента активизации вредных свойств программы (для использования вредоносной программы); с момента передачи третьему лицу или совершения действий, направленных на массовое предоставление доступа к ней (для распространения вредоносной программы).

Субъект создания, использования и распространения вредоносных компьютерных программ.

Субъект преступления, предусмотренного ч. 1 ст. 273 УК РФ, общий – вменяемое физическое лицо, достигшее возраста 16 лет. Субъект преступления, предусмотренного ч. ч. 2, 3 ст. 273 УК РФ, – как общий, так и специальный, а именно лицо, использующее свое служебное положение.

Субъективная сторона создания, использования и распространения вредоносных компьютерных программ.

Описываемый нами состав преступления характеризуется только прямым умыслом, на что указывает слово «заведомо».

Квалифицированные виды создания, использования и распространения вредоносных программ и иной вредоносной информации характеризуются следующими признаками:

– совершение группой лиц по предварительному сговору или организованной группой;

– совершение лицом с использованием своего служебного положения;

– причинение крупного ущерба (свыше 1 000 000 рублей);

– совершение из корыстной заинтересованности;

– наступление тяжких последствий или создание угрозы их наступления.

Содержание квалифицирующих признаков соответствует признакам, описанным при характеристике ст. 272 УК РФ. В частности, по признаку корыстной заинтересованности может быть квалифицирована блокировка вирусом загрузки Windows, сопровождающаяся требованием перевести денежные средства как условием разблокировки (ч. 2 ст. 273 УК РФ).

§ 3. Уголовно-правовая характеристика нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ) и неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ)

Борьба с цифровыми преступлениями осуществляется также посредством применения ст. 274 УК РФ, которая посвящена уголовно-правовой защите от нарушения правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшего уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившего крупный ущерб.

Объект нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Непосредственным объектом данного преступления является безотказная работа информационной системы или сети в соответствии с волей собственника.

Предмет нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей представляют:

1) средства хранения, обработки или передачи компьютерной информации;

2) информационно-телекоммуникационные сети;

3) оконечное оборудование.

Средства хранения, обработки или передачи компьютерной информации – это обобщенное понятие, которое включает аппаратные средства, обеспечивающие манипуляции с информацией. К ним относятся:

– компьютеры (ЭВМ);

– система ЭВМ;

– серверы, облачные банки данных, коммуникаторы, носители информации и т. д.

Информационно-телекоммуникационная сеть – это технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Оконечное оборудование – это оборудование, преобразующее пользовательскую информацию в данные для передачи по линии связи и осуществляющее обратное преобразование.

Объективная сторона нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Объективная сторона преступления выражена в нарушении правил эксплуатации или правил доступа, в двойных последствиях в виде уничтожения, блокирования, модификации либо копирования компьютерной информации и крупном ущербе, а также в причинной связи между совершенным нарушением правил и наступившими последствиями.

Преступление может совершаться как действием (в прямом нарушении правил эксплуатации и доступа), так и бездействием (в несоблюдении или в ненадлежащем соблюдении указанных правил). Диспозиция ст. 274 УК РФ является бланкетной, поэтому для уяснения ее содержания требуется обращение к конкретным инструкциям и правилам, устанавливающим порядок работы со средствами хранения, обработки или передачи охраняемой компьютерной информации, информационно-телекоммуникационными сетями и оконечным оборудованием в ведомстве и организации.

В научной литературе отмечается, что по уровню действия можно выделить следующие правила:

1) правила информационной безопасности, закрепленные в федеральных и ведомственных нормативных актах;

2) правила эксплуатации используемых технических и программных средств;

3) правила эксплуатации и доступа к информационной системе, определенные в конкретной организации или учреждении[27].

Для вменения в обязанность соблюдать правила они должны быть доведены ответственному работнику письменно в отдельном документе или в должностной инструкции, подготовленных правомочным лицом организации или учреждения.

Для наступления ответственности по ст. 274 УК РФ необходимо, чтобы такое нарушение правил эксплуатации или доступа повлекло наступление двух взаимосвязанных последствий. При этом общественно опасные последствия заключаются в одновременном наличии двух факторов:

1) уничтожении, блокировании, модификации или копировании компьютерной информации;

2) наступлении через это крупного ущерба (сумма свыше одного миллиона рублей).

Крупный ущерб может выражаться как в реальном ущербе (уничтожении аппаратной части, базы данных или контента), так

[27] Уголовное право Российской Федерации. Особенная часть : учебник / под ред. проф. М. В. Бавсуна. С. 534.

и в упущенной выгоде (прекращении функционирования информационной системы, отказе в оказании услуг).

Между фактом нарушения и наступившим крупным ущербом должна иметься прямая причинная связь, а также должно быть доказано, что наступившие последствия являются результатом нарушения соответствующих правил, а не программной ошибкой или результатом неправомерных действий других лиц либо действия вредоносной программы.

Субъект нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Субъект преступления, предусмотренного ст. 274 УК РФ, специальный – вменяемое физическое лицо, достигшее ко времени совершения преступления 16-летнего возраста, обязанное соблюдать правила эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, информационно-телекоммуникационных сетей, оконечного оборудования и правил доступа к информационно-телекоммуникационным сетям. Такая обязанность возникает у лица, осведомленного о соблюдении соответствующих правил и имеющего правомерный доступ к информационной системе или сети вследствие выполнения должностных обязанностей по их обслуживанию или получения полезных свойств в качестве пользователя системы.

Субъективная сторона нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Субъективная сторона данного преступления характеризуется как умышленной формой вины (прямой или косвенный умысел направлен на нарушение соответствующих правил), так и неосторожной (например, установка программы без предварительной проверки на наличие в ней компьютерного вируса, которая повлекла нарушение работы компьютера или сети).

Законодатель также предусмотрел квалифицированный вид рассматриваемого нами состава преступления. Речь идет о случаях нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей, повлекших тяжкие последствия или создавших угрозу их наступления. Соответственно, в таких случаях речь идет как о материальном, так и формальном составе преступления. Кроме того, если в результате нарушения описанных правил тяжкие последствия не наступили, а возникла только угроза их наступления, то в таких случаях нужно вести речь только об умышленной форме вины.

Теперь обратим внимание на уголовно-правовую характеристику ст. 274.1 УК РФ, согласно которой уголовно наказуемым признается

неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации.

Статья 274.1 УК РФ введена в июле 2017 г. для защиты критической информационной инфраструктуры Российской Федерации от компьютерных атак[28]. Диспозиция ст. 274.1 является бланкетной и требует обращения к Федеральному закону от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»[29], где раскрываются основные понятия и термины.

Объект неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации.

Непосредственным объектом данного преступления выступает безопасность функционирования критической информационной инфраструктуры России.

Предметом преступления являются объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия этих объектов. Объекты критической информационной инфраструктуры представляют собой информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления, функционирующие в ключевых сферах: здравоохранения, науки, транспорта, связи, энергетики, банковской и иных сферах финансового рынка, топливно-энергетического комплекса, атомной энергии, оборонной и ракетно-космической промышленности, горнодобывающей, металлургической и химической промышленности. Формальным критерием отнесения объекта к критической информационной структуре является включение его в реестр значимых объектов критической информационной инфраструктуры.

Объективная сторона неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации.

Объективная сторона рассматриваемого нами состава преступления заключается в неправомерном воздействии на критическую информационную инфраструктуру Российской Федерации и выражена в трех основных составах:

---

[28] О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» : Федер. закон № 194-ФЗ : принят Гос. Думой 12 июля 2017 года : одобрен Советом Федерации 19 июля 2017 года : послед. ред. // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_220891/ (дата обращения: 20.03.2023).

[29] О безопасности критической информационной инфраструктуры Российской Федерации : Федер. закон № 187-ФЗ : принят Гос. Думой 12 июля 2017 года : одобрен Советом Федерации 19 июля 2017 года : послед. ред. // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения: 20.03.2023).

1) создание, использование, распространение вредоносных компьютерных программ (ч. 1 ст. 274.1 УК РФ);

2) неправомерный доступ к компьютерной информации (ч. 2 ст. 274.1 УК РФ);

3) нарушение правил эксплуатации или правил доступа (ч. 3 ст. 274.1 УК РФ).

Если мы говорим о ч. 1 данной статьи, то преступное деяние выражается в совершении активных действий: в создании, распространении, использовании компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации. Определенную сложность на практике представляет установление признака «заведомость», который предполагает, что вредоносная программа или информация создавалась или использовалась только для воздействия на критическую информационную инфраструктуру, и этот факт охватывался умыслом виновного.

Состав формальный: преступление считается оконченным с момента совершения любого из альтернативных действий.

Если обратиться к объективной стороне ч. 2 ст. 274.1 УК РФ, то можно заключить, что деяние данного преступления выражается в неправомерном доступе к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации. Деяние может выражаться в использовании компьютерных программ (иной компьютерной информации), заведомо предназначенных для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, или иных вредоносных компьютерных программ, что охватывается диспозицией и дополнительной квалификации по ч. 1 ст. 274.1 УК РФ и ст. 273 УК РФ не требует.

При этом данный состав следует признавать материальным, поскольку законодатель предусмотрел в этом случае необходимость установления общественно опасного последствия в виде причинения вреда критической информационной инфраструктуре Российской Федерации и, соответственно, причинно-следственной связи между деянием и последствием. Последствие в виде вреда критической информационной инфраструктуре относится к оценочным категориям, значение его в законе не определено, и правоприменитель должен в каждом конкретном случае устанавливать наличие такого вреда. Обязательным моментом является то, что вред наносится объектам критической информационной инфраструктуры или сети электросвязи и выражается в повреждении или блокировании их работы. Наступившие социальные последствия,

связанные с причинением ущерба или вреда, могут быть квалифицированы как тяжкие последствия.

Поскольку состав преступления, предусмотренный ч. 2 ст. 274.1 УК РФ, материальный, то преступление окончено с момента причинения вреда критической информационной инфраструктуре Российской Федерации.

Если говорить об объективной стороне ч. 3 ст. 274.1 УК РФ, то деяние данного состава преступления выражается в нарушении правил эксплуатации или доступа к объектам критической информационной инфраструктуры Российской Федерации, последствия – в виде вреда критической информационной инфраструктуре Российской Федерации и причинной связи между совершенным нарушением правил и наступившими последствиями. Соответственно, данный состав относится к категории материальных. Преступление может совершаться как действием (умышленное нарушение), так и бездействием (несоблюдение или ненадлежащее соблюдение указанных правил).

Диспозиция ч. 3 ст. 274.1 УК РФ является бланкетной, поэтому для уяснения содержания правил требуется обращение к конкретным нормативным правовым актам. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой законом компьютерной информации может быть осуществлено путем активного действия (например, использование мощностей служебной вычислительной техники для майнинга криптовалюты) или бездействия (что может выражаться в отсутствии обязательного резервного копирования баз данных). Нарушение правил доступа может выражаться в передаче своего логина или пароля третьим лицам.

Субъект неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации.

Субъект составов преступлений, предусмотренных ч. ч. 1, 2 ст. 274.1 УК РФ, является общим – это лицо, достигшее 16 лет. А по ч. 3 названной статьи субъект является специальным: в уголовном законе речь идет о вменяемом физическом лице, достигшем 16-летнего возраста, на которое возложена обязанность соблюдать правила эксплуатации и правила доступа вследствие выполнения профессиональной деятельности по обслуживанию компьютерных систем или сетей (программисты, системные администраторы и т. д.) или вследствие получения правомерного доступа к системе или сетям в качестве пользователя.

Субъективная сторона неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации.

Субъективная сторона преступления, предусмотренного ч. 1 ст. 274.1 УК РФ, характеризуется только прямым умыслом (в отличие от ч. 2 данной статьи, которая характеризуется как прямым, так и косвенным умыслом).

В свою очередь, ч. 3 ст. 274.1 УК РФ характеризуется как умыслом, так и неосторожностью.

Квалифицированные виды неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации характеризуются следующими признаками:

– совершение группой лиц по предварительному сговору или организованной группой;

– совершение лицом с использованием своего служебного положения;

– наступление тяжких последствий.

Содержание квалифицирующих признаков не отличается от аналогичных признаков, предусмотренных ст. ст. 272–274 УК РФ.

§ 4. Уголовно-правовая характеристика преступлений, совершаемых в сфере оборота цифровых активов (криптовалюты) (на примере ст. ст. 205.1, 290 УК РФ)

В настоящее время все чаще правоприменительная практика сталкивается с такими случаями террористической деятельности, как ее финансирование. При этом, как отмечают представители Росфинмониторинга, с развитием цифровых технологий террористическое финансирование все чаще осуществляется посредством использования информационно-телекоммуникационного пространства[30]. В этой связи обращение к уголовно-правовой характеристике такого состава преступления, как финансирование терроризма, в рамках работы, посвященной преступлениям, совершаемым с использованием информационных (цифровых) технологий, является обоснованным и актуальным.

В ранее проводимом нами научном исследовании мы отмечали, что самостоятельная (отдельная) норма в области финансирования террористической деятельности в уголовном законодательстве отсутствует[31]. Однако о финансировании терроризма можно говорить в рамках ст. 205.1 УК РФ («Содействие террористической деятельности»). Правоприменительная практика свидетельствует о том, что финансирование терроризма может быть реализовано посредством

[30] Росфинмониторинг фиксирует факты финансирования терроризма с использованием криптовалют // ТАСС : сайт. URL: https://tass.ru/ekonomika/10978989?ysclid=lmab3xthbe784153136 (дата обращения: 24.02.2023).

[31] Сидорова, Е. З. Уголовно-правовое противодействие финансированию экстремистской деятельности и терроризма : монография. Иркутск, 2023. С. 29.

передачи заинтересованным лицам помимо наличных денежных средств безналичных ценностей, цифровых прав, цифровой валюты и т. п.

В свою очередь, криптовалюта может также присутствовать при совершении такого преступления, как получение взятки (ст. 290 УК РФ). В литературе неоднократно подчеркивалось, что в настоящее время судебная практика[32] и научное сообщество[33] склоняется к тому, чтобы признавать криптовалюту в качестве иного имущества как предмета взяточничества («имущество в электронной форме»). Однако до конца данный вопрос еще не решен, поскольку в настоящее время не в полном объеме определена правовая природа криптовалюты.

По нашему мнению, те или иные информационные (цифровые) технологии могут выступать как предметом, так и средством раскрываемых нами составов преступлений. Для передачи тех или иных ценностей, выступающих предметом финансирования экстремистской деятельности и терроризма, преступники зачастую используют современные цифровые технологии, в том числе сети Интернет, Даркнет, пользуются мессенджерами и т. п.

Если мы рассматриваем современные цифровые технологии в качестве *предмета* обозначенных составов преступлений, то подчеркнем, что в этом случае можно вести речь о:

– безналичных денежных средствах;

– цифровых правах;

– цифровой валюте.

Данные цифровые ценности могут быть использованы в целях финансирования терроризма и отчисляться как систематически, так и разово взноситься в общую кассу, могут быть использованы для приобретения недвижимости или оплаты стоимости ее аренды, могут предназначаться для подкупа должностных лиц и т. д.

Раскроем каждое из представленных понятий.

Определение понятия «безналичные денежные средства» часто вызывает дискуссии, поскольку закрепленного в законе определения данного термина в настоящее время нет. Согласно одному из научных определений, под безналичными денежными средствами можно понимать

---

[32] Суд впервые признал криптовалюту имуществом // Российский медиахолдинг «РБК» : сайт. URL: https://www.rbc.ru/finances/07/05/2018/5af0280d9a7947165a6e8c22?ysclid=lmaeguk8vq139837849. Дата публикации: 07.05.2018.

[33] Асатрян, Х. А., Христюк, А. А. Проблемы определения предмета взяточничества и особенности его выявления в современных реалиях // Всероссийский криминологический журнал : науч. журн. 2022. Т. 16. № 3. С. 377.

денежные средства на банковских счетах, используемые для оплаты, взаимных расчетов посредством перечислений с одного счета на другой[34].

В свою очередь, определение понятия «цифровые права» представлено в действующем законодательстве. Согласно статье 141.1 Гражданского кодекса Российской Федерации[35], цифровыми правами признаются названные в таком качестве в законе обязательственные и иные права, содержание и условия осуществления которых определяются в соответствии с правилами информационной системы, отвечающей установленным законом признакам.

Иными словами, цифровыми правами можно признать только те права, которые названы в качестве таковых в том или ином нормативном правовом акте. При этом распоряжаться цифровыми правами можно только в информационной системе.

Под цифровой валютой, согласно Федеральному закону от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации»[36] (далее – Федеральный закон № 259-ФЗ), следует понимать совокупность электронных данных (цифрового кода или обозначения), содержащихся в информационной системе, которые предлагаются и (или) могут быть приняты в качестве средства платежа, не являющегося денежной единицей Российской Федерации, денежной единицей иностранного государства и (или) международной денежной или расчетной единицей, и (или) в качестве инвестиций и в отношении которых отсутствует лицо, обязанное перед каждым обладателем таких электронных данных, за исключением оператора и (или) узлов информационной системы, обязанных только обеспечивать соответствие порядка выпуска этих электронных данных и осуществления в их отношении действий по внесению (изменению) записей в такую информационную систему ее правилам.

Наиболее популярна в настоящее время такая цифровая валюта, как криптовалюта (и ее основное расчетное средство – биткойн).

---

[34] Семенов, С. К. Деньги: безналичные расчеты в экономике // Финансы и кредит : науч. журн. 2007. № 27 (267). С. 22.

[35] Гражданский кодекс Российской Федерации (часть первая) : ГК : принят Гос. Думой 21 октября 1994 года : послед. ред. // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_5142/ (дата обращения: 13.12.2022).

[36] О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации : Федер. закон № 259-ФЗ : принят Гос. Думой 22 июля 2020 года : одобрен Советом Федерации 24 июля 2020 года : послед. ред. // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_358753/ (дата обращения: 21.06.2023).

Согласно одному из определений, криптовалюта – это цифровой актив и в то же время платежная система, которая использует криптографическую функцию для шифрования записей[37]. В основе криптовалют лежит технология блокчейн (от англ. *blockchain*, изначально *block chain* – «цепь из блоков»). Данная технология подразумевает ведение определенного реестра (списка), состоящего из цепочки блоков. Внутри каждого блока хранится цифровая информация о движении криптовалюты (транзакции). Каждый последующий блок связан с предыдущим. Эта последовательность не может быть нарушена или видоизменена, иначе данные в сети криптовалюты станут недействительны.

В целом суть криптовалюты заключается в том, что она существует только виртуально. Это не «живые» наличные деньги, а определенная комбинация цифр. Каждая такая комбинация представляет собой в некотором роде монету. Для того чтобы выработать (заработать) одну такую комбинацию цифр (монету), требуется длительное машинное (компьютерное) вычисление. Данная вычислительная деятельность осуществляется только в случае бесперебойного постоянного подключения к электросети и сети Интернет. Деятельность по добыванию криптовалюты (по вычислению комбинации цифр и обеспечению бесперебойной работы сети) называется майнинг. Именно с этой целью создаются майнинг-фермы, т. е. происходит объединение нескольких устройств для одновременной добычи криптовалюты (несколько специальных машин для майнинга работают в одном месте и принадлежат, как правило, одному человеку).

Криптовалюта считается альтернативой фиатным деньгам, которые выпускаются государством.

Помимо биткойна в настоящее время существуют и иные виды криптовалюты:

– альткоин;

– эфириум;

– шиткоин;

– токен и др.

Каждый из данных видов криптовалюты обладает своими характерными особенностями и собственной историей возникновения и развития. Например, шиткоин был выпущен мошенниками. Подобная виртуальная монета ничем не обеспечена, поэтому данный термин (шиткоин) также применяют к бесперспективной криптовалюте.

---

[37] Все что важно знать о криптовалюте. Словарь терминов // Российский медиахолдинг «РБК» : сайт. URL: https://www.rbc.ru/crypto/news/5f95b6d79a7947d04d2375e0 (дата обращения: 20.08.2023).

В Федеральном законе № 259-ФЗ также используется термин «цифровые финансовые активы» – это цифровые права, включающие денежные требования, возможность осуществления прав по эмиссионным ценным бумагам, права участия в капитале непубличного акционерного общества, право требовать передачи эмиссионных ценных бумаг, которые предусмотрены решением о выпуске цифровых финансовых активов в порядке, установленном законодательством, выпуск, учет и обращение которых возможны только путем внесения (изменения) записей в информационную систему на основе распределенного реестра, а также в иные информационные системы.

Если мы рассматриваем современные цифровые технологии в качестве *средства и способа* обозначенных составов преступлений, то подчеркнем, что в этом случае можно вести речь о следующем.

Лицо, принявшее решение профинансировать террористическую деятельность или передать взятку должностному лицу, может сделать это различными способами, в том числе передать те или иные товары и ценности лично в руки террориста или коррупционера. Однако современные технологии позволяют осуществить подобную преступную деятельность и другими способами. Можно воспользоваться информационно-телекоммуникационными сетями Интернет, Даркнет. Можно договориться о деталях финансовой помощи террористам или тонкостях совершаемого подкупа посредством мессенджеров WhatsApp, Viber, Telegram и т. п. Можно условиться о встрече через такие социальные сети, как «Одноклассники», «ВКонтакте» и т. п. Существует возможность воспользоваться мобильными телефонами или переговорить с помощью приложения Skype, FaceTime и т. п. Можно осуществить перевод денежных средств через приложения различных банков, через систему «Клиент-Банк», WebMoney, Яндекс.Деньги и т. п.

Иными словами, цифровые технологии, используемые преступниками, – понятие нечеткое, размытое. И связано это с тем, что на данный момент нет единого понятия цифровых технологий. Представляется, что в настоящее время возможности цифровых технологий безграничны, что не может не использоваться для совершения тех или иных преступлений, в том числе финансирования террористической деятельности и совершения взяточничества. Раскрыть все современные цифровые технологии не представляется возможным в силу объективных причин, поскольку наука не стоит на месте, каждый день появляются все новые и новые финансовые приложения, платежные системы, иные информационные технологии, которые могут быть использованы в качестве средства совершения преступлений,

предусмотренных ст. ст. 205.1 и 290 УК РФ. Обратим внимание на наиболее распространенные способы и средства, способствующие совершению финансирования терроризма и взяточничества.

1. Криптовалюта как платежная система.

В научной литературе справедливо отмечается, что введение криптовалюты (которая является одновременно и средством платежа, и системой приема данных платежей) «реализовало идею создания прямых платежей между интернет-пользователями, что практически исключает возможность отследить процесс передачи средств от одного лица другому. Любые посредники в виде банковских или платежных систем исключаются. Анонимность системы криптовалюты практически исключает для государства возможность контроля финансовых потоков»[38]. Это означает, что криптовалюта может сделать экономику террора и коррупцию полностью независимыми от легальных экономических структур, способствуя их латентности. Именно поэтому в настоящее время большое внимание со стороны государства должно быть уделено вопросам предупреждения финансирования терроризма и совершения взяточничества, совершаемых посредством цифровых технологий, поскольку ключевая опасность в данном случае заключается в невозможности со стороны властных структур эффективно противодействовать терроризму и коррупции.

2. Даркнет.

Еще одно цифровое средство, способствующее финансированию терроризма и взяточничеству, требующее внимательного изучения, – это Даркнет. Согласно общедоступной информации, Даркнет – это скрытая сеть, соединения которой устанавливаются только между доверенными лицами. Это анонимная сеть, которая представляет собой систему не связанных между собой виртуальных туннелей, посредством которых информация передается в зашифрованном виде. Главное отличие Даркнета – анонимность и невозможность установления IP-адреса. Данное свойство Даркнета позволяет пользователям не бояться государственного вмешательства и контроля. Именно поэтому Даркнет часто воспринимается как инструмент для осуществления той или иной нелегальной деятельности.

3. Мессенджеры WhatsApp, Viber, Telegram и т. д.

Под термином «мессенджер» специалисты понимают специальную программу для телефона, которая позволяет оперативно обмениваться

[38] Сальников, Е. В., Сальникова, И. Н. Криптовалюта как инновация экономики террора // Вестник евразийской науки : электр. науч. журн. 2016. Т. 8. № 3. С. 4. URL: https: // cyberleninka.ru/article/n/kriptovalyuta-kak-innovatsiya-ekonomiki-terrora?ysclid=lru3og0sjx234867538 (дата обращения: 26.01.2024).

сообщениями, звонить и общаться по видеосвязи через Интернет[39]. Мессенджеры позволяют людям устанавливать и сохранять контакты во всех уголках мира. Однако, как и любое другое изобретение, правонарушители могут использовать мессенджеры для совершения преступлений. Согласно современным исследованиям, наиболее распространенным мессенджером является Viber (у сервиса свыше 200 миллионов пользователей в 193 странах). А самым защищенным и безопасным признается Telegram с активированным секретным чатом[40].

4. Социальные сети «Одноклассники», «ВКонтакте» и т. п.

Социальная сеть – это онлайн-платформа, которая используется для общения, знакомств, выстраивания отношений между людьми со схожими интересами[41]. Социальные сети часто используются как рекламные площадки для демонстрации предлагаемого товара или оказываемых услуг. На данных интернет-платформах организаторы часто предоставляют возможность пользователям слушать музыку, просматривать фильмы и видеоролики, выкладывать фотографии и т. п. Наиболее популярны в настоящее время такие социальные сети, как «Одноклассники», «Вконтакте» и т. д. Как и другие цифровые (информационные) проекты и технологии, социальные сети часто используются преступниками в целях осуществления нелегальной деятельности. Именно в социальных сетях наиболее часто выявляются лица, объединившиеся по террористическим интересам (или стремящиеся присоединиться к подобным сообществам). При этом знакомство лиц в социальных сетях может привести к переходу к общению в тех или иных группах мессенджеров. Таким образом, различные цифровые технологии могут быть использованы в совокупности, могут дополнять друг друга.

5. Мобильные приложения для видеосвязи Skype, FaceTime и другие.

Под мобильным приложением понимается программное обеспечение, предназначенное для работы на смартфонах, планшетах и других мобильных устройствах. Такие мобильные приложения, как Skype, FaceTime и иные, предназначены в первую очередь для видеосвязи, что является очень удобным в современных условиях жизни социума. Например, Skype признан настоящим мастодонтом мира видеосвязи. Данное приложение было разработано еще в 2003 году. Кроме того, Skype

[39] Стефанова, Н. А., Шматок, К. О. Мессенджеры как цифровой бизнес-инструмент // Карельский научный журнал : науч. журн. 2018. Т. 7. № 2 (23). С. 127.

[40] Гатиятуллин, Т. Р. К вопросу выбора безопасного мессенджера // Наука, техника и образование : науч. журн. 2016. № 1 (19). С. 80.

[41] Левин, Л. М. Социальные сети: основные понятия, характеристики и современные исследования // Проблемы современного образования : науч. журн. 2019. № 4. С. 51.

позволяет обмениваться файлами, изображением, видео, музыкой, а также текстовыми сообщениями, отправлять документы и совершать аудио- и видеозвонки. В свою очередь, FaceTime является технологией видео- и аудиозвонков, включающей одноименную веб-камеру, разработанную компанией Apple. Иными словами, FaceTime обладает теми же функциями, что и другие мобильные приложения для видеозвонков, однако ориентир взят именно на владельцев сотовых телефонов фирмы Apple.

Большинство мобильных приложений для видеосвязи имеют функцию создания групповых чатов с возможностью подключения до нескольких сотен человек. При этом поддержка разных платформ позволяет созваниваться и с ноутбука, и с планшета, и со смартфона.

Данными функциями активно пользуются преступники, вовлекающие в преступные сети все новых членов, готовых совершать те или иные уголовно наказуемые деяния.

6. Банковская услуга – система «Клиент-Банк».

Согласно общедоступной информации, система «Клиент-Банк» – это программный комплекс, позволяющий клиенту совершать операции по счету, обмениваться документами и информацией с банком без посещения офиса кредитной организации. Обмен информацией происходит через телефон и компьютер[42]. Главным достоинством данной системы признается отказ от необходимости постоянного посещения банка для совершения той или иной финансовой операции (простота, доступность, скорость). Зачастую система «Клиент-Банк» дает гражданину возможность отслеживать текущее положение его счетов и прогнозировать расходы и прибыль. В круглосуточном режиме клиент может получить выписки по счетам и отслеживать действующих контрагентов.

7. Электронные платежные системы WebMoney, Яндекс.Деньги, Qiwi и т. п.

Система электронных платежей (или электронная платежная система) – это система расчетов между финансовыми организациями, бизнес-организациями и интернет-пользователями при покупке-продаже товаров и услуг через Интернет. Ключевым отличием электронных платежных систем от счетов в банках является отсутствие в первом случае банковских пластиковых карт. Существуют лишь виртуальные карты, позволяющие проводить все финансовые транзакции через Интернет. Такую карту легче приобрести, поскольку ее выпуск осуществляется без проверки личности владельца. С другой стороны, такие карты, как

[42] Система «Клиент-Банк» // Banki.ru : сайт. URL: https://www.banki.ru/wikibank/sistema_klient-bank/?ysclid=l8siq0dfxu208243989 (дата обращения: 28.08.2023).

правило, не предусматривают возможности пополнения счета, и они менее защищены от преступных посягательств. Возможность скрыть свою личность при использовании электронных платежных систем в определенной мере способствует осуществлению нелегальных транзакций, в том числе в целях финансирования экстремизма и терроризма.

Таким образом, можно заключить, что в настоящее время существует большое количество цифровых инструментов, помогающих правонарушителям совершать преступления, в том числе посредством тех или иных цифровых технологий осуществлять финансирование террористической деятельности и передачу предмета взятки. Опасность данного явления заключается в том, что государство на современном этапе не может оказывать эффективное противодействие подобным цифровым преступлениям как по объективным, так и субъективным причинам.

Однако подчеркнем, что прежде чем использовать криптовалюту в своих преступных целях, террористы и представители киберкриминала всегда оценивают свои риски. И если 6–8 лет назад представители террористических организаций и организованной преступности скептически относились к возможностям использования криптовалюты, то в настоящее время цифровая валюта используется преступниками повсеместно. Прежняя позиция была основана на следующих тезисах, которые озвучивали эксперты Европарламента:

– террористы и другие преступники с подозрением относятся к криптовалютам, поскольку считают, что биткойн специально создан ФБР для возможности их выявления и раскрытия их преступной деятельности;

– многие представители террористических организаций, в первую очередь их руководители, – это люди старшего возраста (40–50 лет), которые не всегда понимают суть криптовалюты и, соответственно, испытывают к ней недоверие;

– представители организованной преступности и террористы видят особо пристальный интерес международных и национальных финансовых организаций и правоохранительных структур к сфере криптовалют, вследствие чего не хотят оказаться в поле зрения их интересов[43].

Сейчас ситуация изменилась. Террористы и представители организованной преступности видят, как развивается сфера цифровых технологий и особенно сфера финансов. Ни для кого не секрет, с каким количеством технических, юридических, организационных, материальных, кадровых трудностей сталкиваются представители правоохранительных

[43] Криптовалюта, блокчейн и преступность // Livejournal : сайт. URL: https://sell-off.livejournal.com/27856173.html?ysclid=lmaanwxby896569801 (дата обращения: 24.02.2023).

органов для того, чтобы выявить проводимые транзакции криптовалюты. Именно по этой причине в настоящее время для террористов и представителей организованной преступности использование криптовалюты остается по-прежнему привлекательным и актуальным. Однако общественные отношения не стоят на месте, они развиваются. Развивается и государственная политика в области противодействия цифровым преступлениям, в том числе финансированию террористической деятельности посредством криптовалюты. Как подчеркивают специалисты, актуальные, отвечающие современным реалиям и требованиям безопасности правовые предписания, касающиеся работы криптобирж, заставят последних более внимательно относиться к проводимым транзакциям, поскольку в противном случае возможно будет привлечь к ответственности не только самих преступников, использующих криптовалюту в преступных целях, но и представителей криптобирж за то, что последние допустили использование криптовалюты в криминальных целях[44].

В следующей главе нашего пособия мы обратимся к анализу современной уголовной политики в сфере обеспечения цифровой безопасности.

[44] Мурадян, С. В. Перспективы использования криптовалют для целей финансирования терроризма и меры по предупреждению указанной тенденции // Закон и право : науч. журн. 2022. № 5. С. 198.

ГЛАВА 3.
УГОЛОВНАЯ ПОЛИТИКА
В СФЕРЕ ОБЕСПЕЧЕНИЯ ЦИФРОВОЙ БЕЗОПАСНОСТИ

§ 1. Понятие уголовной политики в сфере обеспечения цифровой безопасности

В научной литературе отсутствует единство мнений относительного того, что следует понимать под термином «уголовная политика». Согласно одному из определений, под уголовной политикой можно понимать государственную деятельность, которая направлена на закрепление в уголовном законе и иных нормативных правовых актах установок, определяющих преступность общественно опасных деяний, способы и пределы наказуемости таких деяний и других мер уголовной ответственности за совершение общественно опасных деяний, и результат данной деятельности[45].

Знакомясь с научными исследованиями по проблеме уголовной политики, можно прийти к заключению о существовании незавершенной дискуссии относительно того, какие направления уголовной политики должны выделяться, какое определение данного понятия целесообразнее использовать, что следует относить к объектам и субъектам уголовной политики и т. д. Однако настоящая работа направлена не на то, чтобы продолжить ведение данной научной дискуссии, и не на то, чтобы претендовать на исключительно правильное формулирование тех или иных понятий и определений. Ключевая задача нашего пособия заключается в том, чтобы дать общее представление о современной уголовной политике в области противодействия преступлениям, совершаемым с использованием информационных (цифровых) технологий.

Можно выделить общее направление уголовной политики, реализуемой в стране, и специальные направления уголовной политики, затрагивающей ту или иную область общественных отношений.

Исследуя сферу цифровой преступности, можно выделить такое направление уголовной политики, как уголовная политика в сфере обеспечения цифровой безопасности.

Опираясь на ранее проведенные научные исследования[46], можно заключить, что под уголовной политикой в сфере обеспечения цифровой

[45] Сидорова, Е. З., Босхолов, С. С. Уголовная политика в сфере образования // Академический юридический журнал : науч. журн. 2021. Т. 22. № 3 (85) С. 255.

[46] Сидорова, Е. З. Принципы и значение уголовной политики в сфере предупреждения преступности в образовательной среде // Сибирское юридическое обозрение : науч. журн. 2021. Т. 18. № 4. С. 424.

безопасности следует понимать целенаправленную деятельность государственных органов, органов местного самоуправления и иных субъектов, ориентированную на борьбу с преступлениями, совершаемыми с использованием информационных (цифровых) технологий.

Уголовная политика проявляется в первую очередь в тех нормативных правовых актах, которые принимаются и действуют в настоящее время, а также в судебной и правоприменительной практике. В этой связи целесообразным является обращение к действующей нормативно-правовой базе, затрагивающей сферу противодействия преступлениям, совершаемым с использованием информационных (цифровых) технологий. При этом подчеркнем, что конечной целью применения таких правовых предписаний является обеспечение цифровой безопасности. В научной литературе уделено пристальное внимание вопросу о содержании термина «цифровая безопасность». И поскольку в настоящее время на законодательном уровне содержание данного понятия не закреплено, под цифровой безопасностью можно понимать состояние защищенности цифровой информации, цифровой инфраструктуры и цифровых технологий, обеспечивающее защиту конституционных прав и свобод человека и гражданина, законных интересов субъектов цифровых правоотношений от реальных и потенциальных угроз[47].

§ 2. Влияние законодательного регулирования на преступность в сфере информационных (цифровых) технологий

Говоря о регулировании такой сферы общественной жизни, как цифровые отношения, нужно отметить, что они зародились относительно недавно (не с момента возникновения человечества, а лишь с развитием технологий). При этом технологический процесс, как известно, всегда опережает законодателя. Можно констатировать, что в большинстве случаев законодатель не действует на опережение, он лишь позволяет себе тем или иным образом регулировать уже сложившиеся общественные отношения. Не является исключением и сфера цифровых отношений.

Вместе с тем, несмотря на то, что законодатель зачастую действует «с опозданием», нельзя не отметить, что достаточно сильно его влияние на развитие цифровых отношений, в том числе цифровой преступности. Подчеркнем, что в научной литературе используются такие термины, как «преступления в сфере оборота цифровых активов», «преступления,

[47] Бегишев, И. Р. Семантический анализ термина «цифровая безопасность» // Юрислингвистика : науч. журн. 2021. № 20 (31). С.35.

совершаемые с использованием IT (интернет вещей)»[48] и другие. Несмотря на то, что данные понятия имеют определенные особенности и специфические характеристики, в целом речь идет о цифровой преступности.

Влияние законодательного регулирования на преступность в сфере информационных (цифровых) технологий проявляется в первую очередь в том, что те или иные деяния признаются преступными только с того момента, как их законодательная модель (уголовно-правовая конструкция) находит свое закрепление в действующем уголовном законе. Иными словами, для того чтобы признать те или иные действия людей в цифровой сфере преступными, необходимо, чтобы подобный состав преступления был отражен в УК РФ.

Другой аспект влияния законодательного регулирования на преступность в сфере информационных (цифровых) технологий проявляется в том, что на законодательном уровне вообще появляется правовое регулирование цифровых отношений, а значит, появляется возможность говорить о цифровых преступлениях. Так, в 2020 году был принят важнейший Федеральный закон № 259-ФЗ «О цифровых финансовых активах, цифровой валюте …». Несмотря на ряд существенных недостатков, присущих многим нормативным правовым актам, данный документ положил начало регулированию сферы современных цифровых отношений в нашей стране. И в этой связи его значение для правоприменительной практики трудно переоценить.

Разумеется, в области правового регулирования цифровых отношений по-прежнему остается достаточно много «белых пятен», многие вопросы остаются неурегулированными, существуют в правовом поле и некоторые противоречия в данной сфере. Вместе с тем все действующие нормативные правовые акты, так или иначе затрагивающие сферу цифровых отношений, влияют на складывающуюся практику применения правовых норм и установок, на развитие цифровых отношений в целом и, конечно, отражаются на уголовной политике в сфере обеспечения цифровой безопасности.

Таким образом, несмотря на то, что цифровые отношения развиваются независимо от того, предусмотрел ли их законодатель, влияние правовых предписаний на данную сферу жизни социума неизбежно. И в связи с тем, что в обществе появляются цифровые преступления и цифровая преступность, государство вынуждено предпринимать действия, направленные на борьбу с подобным негативным явлением, и проявляться такие действия будут в первую

[48] Ищук, Я. Г., Пинкевич, Т. В., Смольянинов, Е. С. Цифровая криминология : учеб. пособие. М. : Академия управления МВД России, 2021. С. 101.

очередь посредством развития соответствующей уголовной политики в сфере обеспечения цифровой безопасности, о чем мы говорили выше.

Отметим, что современная уголовная политика в сфере обеспечения цифровой безопасности строится на правовых предписаниях следующих нормативных правовых актов.

1) Конституция Российской Федерации 1993 г.[49]

Главный закон страны содержит несколько нормативно-правовых предписаний, затрагивающих область отношений, в которых значимая роль отводится информации. Так, согласно статье 24, сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются. В свою очередь, закрепленное в статье 29 правило гласит, что каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Согласно статье 71, в ведении Российской Федерации находятся вопросы, в том числе связанные с информацией, информационными технологиями и связью, а также с обеспечением безопасности личности, общества и государства при применении информационных технологий, обороте цифровых данных.

Таким образом, можно констатировать, что Конституция позволяет гражданам России осуществлять какую-либо деятельность, связанную с распространением и использованием той или иной информации, однако осуществлять подобную деятельность можно, не нарушая при этом установленные запреты. В противном случае уполномоченные субъекты вправе применить к нарушителю соответствующие меры ответственности.

2) Уголовный кодекс Российской Федерации.

Несомненно, ключевым нормативным правовым актом, на котором строится современная уголовная политика в сфере обеспечения цифровой безопасности, является действующий уголовный закон. Именно названный

---

[49] Российская Федерация. Конституция : принята всенародным голосованием 12 декабря 1993 года с изменениями, принятыми в ходе общероссийского голосования 1 июля 2020 года (в редакции указов Президента Российской Федерации от 09.01.1996 № 20, от 10.02.1996 № 173, от 09.06.2001 № 679, от 25.07.2003 № 841; федеральных конституционных законов от 25.03.2004 № 1-ФКЗ, от 14.10.2005 № 6-ФКЗ, от 12.07.2006 № 2-ФКЗ, от 30.12.2006 № 6-ФКЗ, от 21.07.2007 № 5-ФКЗ; законов Российской Федерации о поправке к Конституции Российской Федерации от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ; Федерального конституционного закона от 21.03.2014 № 6-ФКЗ; Закона Российской Федерации о поправке к Конституции Российской Федерации от 21.07.2014 № 11-ФКЗ; Указа Президента Российской Феде-рации от 27.03.2019 № 130; Закона Российской Федерации о поправке к Конституции Российской Федерации от 14.03.2020 № 1-ФКЗ; федеральных конституционных законов от 04.10.2022 № 5-ФКЗ, от 04.10.2022 № 6-ФКЗ, от 04.10.2022 № 7-ФКЗ, от 04.10.2022 № 8-ФКЗ) // Официальный интернет-портал правовой информации : сайт. URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102027595 (дата обращения: 20.08.2023).

нормативный правовой акт предусматривает те виды преступлений, за совершение которых лицо привлекается к уголовной ответственности, в том числе преступлений цифровой (информационной) направленности.

Ранее мы уже говорили о том, что вопрос о перечне цифровых преступлений (киберпреступлений) до сих пор относится к разряду дискуссионных. На наш взгляд, ключевыми цифровыми преступлениями являются мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ), неправомерный доступ к компьютерной информации (ст. 272 УК РФ), создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ), преступления, совершаемые в сфере оборота цифровых активов (криптовалюты) (например, ст. 205.1 УК РФ – содействие террористической деятельности путем ее финансирования), и другие.

3) Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Данный нормативный правовой акт лежит в основе регулирования таких явлений, как информация, информационные технологии и защита информации. Объемный по своему содержанию, Закон раскрывает основные принципы правового регулирования отношений в сфере информации, освещает обязанности отдельных субъектов данных отношений (таких как оператор поисковой системы, владелец аудиовизуального сервиса и т. д.), раскрывает понятия, в частности информационных систем.

Значимость указанного Закона заключается в том, что он является базовым для регулирования всех складывающихся цифровых отношений в современном обществе. Именно на него опирается правоприменитель в вопросах привлечения лиц к уголовной ответственности за совершение того или иного цифрового преступления (если есть необходимость в определении содержания того или иного термина и понятия из информационной сферы).

4) Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 5 декабря 2016 г. № 646[50].

Указанный нормативный правовой акт является базовым в вопросах обеспечения информационной безопасности нашего государства, раскрывая ключевые понятия в данной области общественных отношений.

[50] Об утверждении Доктрины информационной безопасности Российской Федерации : Указ Президента Российской Федерации от 5 декабря 2016 года № 646 // Официальный интернет-портал правовой информации : сайт. URL: http://pravo.gov.ru/proxy/ips/?docbody=&firstDoc=1&lastDoc=1&nd=102417017 (дата обращения: 20.03.2023).

В названном документе в том числе дается определение понятия «угрозы информационной безопасности Российской Федерации», под которыми понимаются действия и факторы, создающие опасность нанесения ущерба национальным интересам в информационной сфере. К числу таких угроз может быть отнесена и цифровая преступность, подрывающая уровень защищенности информационной сферы жизнедеятельности социума.

Кроме того, названный нормативный правовой акт описывает национальные интересы в информационной сфере, определяет стратегические цели и основные направления обеспечения информационной безопасности, раскрывает организационные основы обеспечения информационной безопасности.

В вопросах обеспечения информационной безопасности действуют также иные нормативные правовые акты, принятые на уровне субъектов Российской Федерации и муниципалитетов. Однако ключевым документом в области реализации уголовной политики в сфере обеспечения цифровой безопасности остается действующий УК РФ. Так, если обратить внимание на вопросы криминализации тех или иных цифровых преступлений, то можно заметить, что в данной сфере наблюдается определенное ужесточение. В частности, в первоначальной версии Кодекса 1996 года отсутствовал такой состав преступления, как мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ). Он появился только в 2012 году: Федеральным законом от 29.11.2012 № 207-ФЗ[51] были внесены соответствующие изменения в УК РФ. Изначально также отсутствовал и такой состав цифрового преступления, как неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ). Данный уголовно-правовой запрет нашел свое отражение в уголовном законодательстве только в 2017 году на основании соответствующих изменений, внесенных Федеральным законом от 26.07.2017 № 194-ФЗ.

Если обратиться к вопросу пенализации цифровых преступлений, то здесь мы также можем наблюдать политику ужесточения уголовной ответственности за их совершение. Например, в первоначальной редакции такого состава преступления, как создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ) (напомним, что изначально наименование данной статьи звучало как «создание, использование и распространение вредоносных программ

[51] О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации : Федер. закон № 207-ФЗ : принят Гос. Думой 23 ноября 2012 года : одобрен Советом Федерации 28 ноября 2012 года : послед. ред. // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_138322/ (дата обращения: 21.06.2023).

для ЭВМ»), законодатель предусматривал максимальное наказание в виде лишения свободы на срок до 3 лет со штрафом (максимальный размер штрафа был равен размеру дохода осужденного за период от 2 до 5 месяцев). В действующей же редакции наказание за совершение названного преступления ужесточилось. Теперь максимальное наказание заключается в лишении свободы на срок до 4 лет со штрафом в размере дохода осужденного за период до 18 месяцев.

Другой пример. Как мы уже говорили, в 2012 году законодатель вводит в УК РФ статью 159.6 – мошенничество в сфере компьютерной информации. И если в первоначальной редакции части 2 указанной статьи (совершение названного преступления группой лиц по предварительному сговору либо с причинением значительного ущерба гражданину) предусматривалась максимальная ответственность в виде лишения свободы на срок до 4 лет, то в настоящее время максимальное наказание заключается в лишении свободы на срок до 5 лет.

На основании изложенного можно судить о явном ужесточении уголовной репрессии за совершение цифровых преступлений.

Положения современной уголовной политики проявляются также в актах судебной практики. Например, на основании нижеприведенного примера можно говорить о том, что правоприменитель настроен применять максимально строгие меры государственного принуждения к лицам, совершившим цифровые преступления. Например, в 2019 году гражданин Ф. обвинялся в совершении совокупности преступлений, в том числе предусмотренных ч. 3 ст. 272, ч. 3 ст. 272, ч. 3 ст. 272, ч. 4 ст. 274.1, ч. 3 ст. 272, ч. 3 ст. 272 УК РФ. Несмотря на то, что только одно из совокупности преступлений, в которых обвинялся гражданин Ф., относилось к категории тяжких преступлений, правоприменителем была избрана для обвиняемого такая мера пресечения, как заключение под стражу. Мотивировалось такое решение тем, что в период содержания гражданина Ф. под стражей следователь должен был провести ряд следственных действий, в том числе осмотреть серверное оборудование, электронные сообщения электронного почтового ящика, персональный компьютер ООО «…», сервер ООО «...», в случае необходимости назначить в отношении указанных компьютеров компьютерно-технические судебные экспертизы, истребовать заключения экспертов по назначенным экспертизам, после получения заключений эксперта осмотреть в полном объеме изъятую компьютерную технику, средства мобильной связи, электронные носители информации и иные изъятые предметы и документы, по которым принять законное и обоснованное решение, выполнить комплекс мероприятий, направленных на проверку причастности Ф. к совершению аналогичных преступлений.

Иными словами, требовалось проведение целого ряда следственных действий, связанных с исследованием «компьютерных» доказательств. При этом обвиняемый Ф. настаивал на том, что считает избранную в отношении него меру пресечения слишком суровой. В своих жалобах он указывал, что его содержали под стражей 6 месяцев по обвинению в совершении преступления средней тяжести, которое он признал в полном объеме, раскаялся в содеянном, сотрудничает с органом следствия, что, с учетом действующего закона и правоприменительной практики, является правовым нонсенсом. Ф. является социально адаптированным лицом, имеет в собственности жилье, в котором зарегистрирован и проживал до задержания, имеет полную семью, 3-месячного сына, супругу, которые нуждаются в его заботе и помощи, что говорит об отсутствии правовых оснований для применения в отношении него максимально суровой меры пресечения в виде содержания под стражей.

Однако суд не согласился с доводами обвиняемого Ф. и продлил ему срок содержания под стражей, объясняя это тем, что, во-первых, Ф. ранее привлекался к уголовной и административной ответственности, во-вторых, он обладает специальными познаниями в современных информационных технологиях и имеет опыт удаленного доступа к компьютерной информации, а значит, может повлиять на ход расследования данного уголовного дела и уничтожить те или иные «компьютерные» доказательства, и в-третьих, все соучастники инкриминируемых ему преступлений не установлены, а свидетель И. и второй обвиняемый О. опасаются давления со стороны Ф.[52]

Подчеркнем, что в правоприменительной практике можно встретить достаточно много примеров привлечения лиц к уголовной ответственности в связи с совершением того или иного цифрового преступления. Например, в 2020 году за совершение совокупности преступлений, предусмотренных п. п. «б», «в» ч. 3 ст. 159.6 УК РФ «Мошенничество в сфере компьютерной информации» (два эпизода), ч. 3 ст. 272 УК РФ «Неправомерный доступ к компьютерной информации» (два эпизода), была осуждена гражданка Д., при этом наказание в виде лишения свободы ей было назначено условно[53]. В этом же году был осужден гражданин К., признанный виновным в совершении преступления, предусмотренного ч. 1 ст. 273 УК РФ

[52] Апелляционное постановление Приморского краевого суда (Приморский край) № 22-5291/2019 22К-5291/2019 от 11 декабря 2019 года по делу № 3/2-355/19 // Судебные и нормативные акты РФ : сайт. URL: https://sudact.ru/regular/doc/W4wm3MOBf2m4/ (дата обращения: 01.09.2023).

[53] Приговор Октябрьского городского суда (Республика Башкортостан) № 1-243/2020 от 29 июля 2020 года по делу № 1-243/2020 // Судебные и нормативные акты РФ : сайт. URL: https://sudact.ru/regular/doc/eLKpELsMEF5w/ (дата обращения: 01.09.2023).

(создание, использование и распространение вредоносных компьютерных программ). Судом он был приговорен к одному году ограничения свободы[54]. В 2020 году также была осуждена гражданка М., совершившая преступление, предусмотренное п. «г» ч. 3 ст. 158 УК РФ (кража с банковского счета, а равно в отношении электронных денежных средств), суд назначил ей наказание в виде лишения свободы сроком на 1 (один) год условно[55].

Из приведенных примеров мы можем заключить, что при назначении наказания лицам, совершившим цифровые преступления, суды нередко назначают наказание в виде условного лишения свободы либо выбирают тот вид наказания для осужденного, который не связан с изоляцией от общества (например, ограничение свободы). В этой связи мы также можем судить об определенной уголовной политике в области обеспечения цифровой безопасности: правоприменитель, учитывая обстоятельства произошедшего, по сути «надеется» на то, что цифровой преступник способен исправиться без реального отбывания наказания.

В следующей главе нашего пособия мы обратимся к вопросу криминологического анализа цифровой преступности.

[54] Приговор Павловского районного суда (Воронежская область) № 1-40/2020 от 25 ноября 2020 года по делу № 1-40/2020 // Судебные и нормативные акты РФ : сайт. URL: https://sudact.ru/regular/doc/KL22CmxCcxU/ (дата обращения: 01.09.2023).

[55] Приговор Подольского городского суда (Московская область) № 1-758/2020 от 9 ноября 2020 года по делу № 1-758/2020 // Судебные и нормативные акты РФ : сайт. URL: https://sudact.ru/regular/doc/t67MABvgc3o0/ (дата обращения: 01.09.2023).

ГЛАВА 4.
КРИМИНОЛОГИЧЕСКИЙ АНАЛИЗ ПРЕСТУПНОСТИ В СФЕРЕ ИНФОРМАЦИОННЫХ (ЦИФРОВЫХ) ТЕХНОЛОГИЙ

§ 1. Понятие преступности в сфере информационных (цифровых) технологий

Обращаясь к исследованию вопросов, связанных с криминологической характеристикой цифровой преступности, отметим, что в научной литературе используются также такие понятия, как «преступность в сфере технологий больших данных», «преступность в сфере оборота криптовалюты», «преступность в сфере искусственного интеллекта», «преступность в сфере IT (интернет вещей)» и другие[56]. Во всех этих случаях подразумевается такое явление, как цифровая преступность (или киберпреступность), хотя данные понятия характеризуются своими особенностями.

Так, технологии больших данных (Big Data) – это разнообразные данные, поступающие в больших объемах и с огромной скоростью, обработать которые при помощи стандартного программного обеспечения достаточно проблематично, поэтому для обработки таких данных требуется использование специальных программ и оборудования. Большие данные можно использовать для решения разных задач (например, для прокладывания маршрутов на картах, составления поисковых запросов, оформления покупок онлайн)[57].

Криптовалюта (цифровые активы) – это совокупность электронных данных (цифрового кода или обозначения), которые содержатся в информационной системе. В действующем законодательстве есть определение понятия «цифровой актив» (Федеральный закон № 259-ФЗ), однако в целом суть данного явления заключается в закреплении определенных цифровых кодов в специальной системе. Вмешательство посторонних лиц с целью внесения тех или иных изменений в такую систему запрещено.

Искусственный интеллект – это способность компьютера обучаться, принимать решения и выполнять действия, свойственные человеческому интеллекту. Основная цель искусственного интеллекта заключается

---

[56] Ищук, Я. Г., Пинкевич, Т. В., Смольянинов, Е. С. Указ. соч. С. 105.

[57] Big Data: что это, где используется и как стать аналитиком больших данных // LPGenerator : сайт. URL: https://lpgenerator.ru/blog/chto-takoe-big-data/?ysclid=lm1h3261q7608694141 (дата обращения: 01.09.2023).

в выполнении творческих функций, которые традиционно считаются прерогативой человека[58].

Интернет вещей (сфера IT) – это множество физических объектов (устройств), подключенных к сети Интернет и обменивающихся данными (например, умные часы, умный дом и т. п.)[59].

Эти и многие другие цифровые определения и термины взаимосвязаны между собой и в конечном итоге, если они так или иначе начинают фигурировать при совершении преступлений (например, в качестве предмета преступного посягательства или средства его совершения), образуют такое явление, как цифровая преступность (или киберпреступность).

С развитием различных технологий мы постепенно привыкли к тому, что Интернет помогает решить большинство наших повседневных задач (например, путем дистанционного доступа в интернет-магазины или необходимого делового общения в формате реального времени), помогает с архивацией личных данных путем их помещения в цифровые хранилища информации, позволяет оперативно использовать банковские карты и т. п. Эти и многие другие составляющие нашей повседневной жизни позволяют охарактеризовать интернет-технологии с положительной стороны. Однако у каждого положительного явления имеются те или иные отрицательные стороны. Например, в тот момент, когда человек размещает информацию о себе в электронных архивах, он становится потенциальной жертвой цифрового преступления. Объясняется это тем, что человек становится уязвимым к совершению в отношении него преступления именно по причине переноса личной информации в Интернет. Тем самым криминогенная ситуация, связанная с цифровым пространством, ухудшается. У преступников с каждым днем появляется все больше новых инструментов, методов и средств для совершения преступлений в цифровой среде.

Актуальность данной темы выражается в том, что с ростом цифровизации в обществе ухудшается криминогенная обстановка в сфере применения информационно-телекоммуникационных технологий (ИТТ). Интернет как инструмент совершения преступления стал почти повсеместно доступным. Процент населения, использующего ИТТ, растет

---

[58] Толковый словарь по искусственному интеллекту / авт.-сост. А. Н. Аверкин, М. Г. Гаазе-Рапопорт, Д. А. Поспелов. М. : Радио и связь, 1992. 256 с. Компьютерная версия: И. Н. Листопад, А. Б. Прокудин, Е. Н. Щербаков // AI Handbook. Справочник «Интеллектуальные системы и искусственный интеллект» : сайт. URL: http://aihandbook.intsys.org.ru/index.php/intro/ai-glossary (дата обращения: 01.09.2023).

[59] Что такое IoT и что о нем следует знать // Хабр : сайт. URL: https://habr.com/ru/companies/otus/articles/549550/ (дата обращения: 01.09.2023).

постоянно, а значит, пропорционально с этим растет количество потенциальных жертв цифровых преступлений, например, растет количество потерпевших от киберпреступлений, связанных с хищением денежных средств с банковских счетов граждан или с неправомерным доступом к компьютерной информации.

Исследование современной цифровой преступности необходимо для того, чтобы определить ее криминологически значимые особенности, при этом в таком исследовании в большей степени должно акцентироваться внимание на изучении криминологических особенностей цифрового преступника и его жертвы. На наш взгляд, в основе такого исследования должны лежать общенаучные методы познания: индукция, дедукция, обобщение, анализ, сравнение и т. п. В качестве основных материалов исследования должны быть определены данные официальной статистики, а также материалы ранее проведенных исследований по аналогичной тематике.

Говоря о понятии преступности в сфере информационных (цифровых) технологий, или цифровой преступности, или киберпреступности, подчеркнем, что в конце прошлого столетия появилось такое понятие, как киберпреступление. В современной научной литературе можно встретить и иные термины: «цифровые преступления», «интернет-преступления», «компьютерные преступления» и т. п. Поскольку в настоящее время в научных кругах еще не устоялась та или иная формулировка описываемого нами явления, отметим, что в настоящей работе данные термины будут использоваться как равнозначные. С другой стороны, определенные отличия у данных терминов присутствуют. Например, если говорить о «компьютерной» преступности, то, как правило, в данном случае подразумевается более узкий круг уголовно наказуемых деяний, чем в случае с термином «цифровая преступность».

Компьютерная преступность – это совокупность компьютерных преступлений, где компьютерная информация является предметом преступных посягательств, а также преступлений, которые совершаются посредством общественно опасных деяний, предметом которых является компьютерная информация. Эти деяния посягают на безопасность сферы компьютерной информации, являются одним из наиболее опасных и вредоносных явлений современного мира[60].

Когда мы говорим о цифровых преступлениях, то, как правило, их предметом выступают персональные данные, а также электронные

[60] Кузнецов, Д. А., Манохина, О. В. Компьютерная преступность // Бюллетень медицинских интернет-конференций : электр. науч. журн. 2015. Т. 5. № 12. С. 1484. URL: https://medconfer.com/node/5584?ysclid=lru41i87i1611569550 (дата обращения: 26.01.2024).

средства платежа. Еще одной чертой данных составов является совершение преступления с использованием компьютерных сетей или же информационно-телекоммуникационных технологий. На фоне глобализации всего цифрового пространства Интернет становится наиболее развитым методом совершения преступлений. Связано это именно с цифровизацией общества и переносом баз данных в цифровое пространство, что, несомненно, является предпосылкой к росту числа киберпреступлений.

Далее раскроем ключевые свойства (признаки) современной цифровой преступности.

§ 2. Преступность в сфере информационных (цифровых) технологий и ее основные свойства (признаки)

Еще раз подчеркнем, что актуальность исследования цифровой преступности обуславливается тем, что с развитием общества растет и его цифровая составляющая, где информационные сети становятся неотъемлемой частью социальной жизни. Причиной роста темпов цифровизации является глобализация нашей планеты, поскольку уже почти у каждого человека есть смартфон либо хотя бы один персональный компьютер или ноутбук с доступом во «всемирную паутину», что также может являться фактором роста преступлений в цифровой сфере. Интернет стал как полезным средством для решения повседневных жизненных задач человека, так и средством совершения преступлений (например, с его помощью можно осуществить неправомерный доступ к компьютерной информации).

Напомним, что преступность – это сложное социально-правовое явление, исторически изменчивое, негативное, представляющее систему преступлений, совершенных на определенной территории за определенный период времени[61].

Преступность характеризуется двумя категориями показателей: *количественными* и *качественными*.

1. Среди количественных показателей выделяются объем преступности, уровень преступности, динамика преступности. Так как данное социально-правовое явление является системным и комплексным, с помощью данных компонентов определяется количественная характеристика преступности на определенной территории за определенный промежуток времени.

[61] Афанасьева, О. Р., Гончарова, М. В., Шиян, В. И. Криминология : учебник и практикум для вузов. М. : Юрайт, 2023. С. 65.

Объем преступности – это сумма всех зарегистрированных преступлений, а также лиц, их совершивших, однако стоит учесть, что количество преступлений может не совпадать с количеством лиц, их совершивших: например, одно лицо совершило совокупность преступлений, преступная организация совершает лишь одно преступление, но лиц, участвовавших в совершении преступления, было больше.

Уровень преступности – это количество преступлений в соотношении с количеством лиц, проживающих на определенной территории, или в относительных величинах. Уровень преступности складывается из нескольких факторов:

– коэффициент преступности;

– коэффициент криминальной активности населения;

– коэффициент виктимности.

Динамика преступности – это изменяющийся показатель, который выводится по временным промежуткам. Например, текущий показатель динамики преступности – это показатель за аналогичный период прошлых лет или показатель, систематично проводимый (например, раз в год).

2. К качественным показателям относятся структура преступности, география преступности, характер преступности и цена преступности.

Главными свойствами *структуры* по признакам преступлений выступают:

– количество рецидивов, количество профессиональной преступности, количество преступлений, совершаемых в составе групп по предварительному сговору и организованных преступных групп, а также количество преступлений, совершенных женщинами, несовершеннолетними и т. п.;

– количество умышленных и неосторожных преступлений;

– количество видов и категорий преступлений.

Следует также учесть, что структура преступности может классифицироваться по характеристике личности преступника, а именно:

– пол лица, совершившего преступное деяние;

– возраст лица, совершившего преступление;

– количество лиц, участвующих в совершении преступлений, и т. д.

География преступности помогает определить, какие преступления чаще всего совершаются в том или ином регионе страны, выделить некие особенности совершения преступлений, а также поспособствовать в разработке методов и средств по противодействию преступности в данных регионах.

Характером преступности является количество наиболее опасных преступлений (тяжких и особо тяжких) в структуре данного явления. Характер преступности также определяется путем сопоставления личности

преступника (например, является ли он рецидивистом, профессиональным преступником и т. п.).

Цена преступности – это количество материального и морального вреда, причиненного преступником его жертвам или близким лицам жертв. Цену преступности следует разделить на несколько видов:

– преступления, нанесшие прямой материальный ущерб;

– преступления, косвенно нанесшие материальный ущерб;

– экономические издержки и иного вида издержки, произведенные в связи с противодействием преступности.

Именно в этом проявляются социальные последствия цифровой преступности. Как отмечают исследователи, «социальные последствия от внедрения цифровых технологий будут ощутимыми, поскольку цифровая преступность будет расти»[62]. Цена цифровой преступности будет все выше, поскольку ежегодно будут расти количественные и качественные показатели такой преступности. И это будет продолжаться до тех пор, пока общество не выработает эффективные меры профилактики и предупреждения цифровых преступлений.

Если обратиться к вопросу о классификации цифровой преступности, то, несомненно, в первую очередь следует говорить о тех цифровых преступлениях, которые составляют структуру названного нами вида преступности. Как мы уже говорили, в основном речь следует вести о таких уголовно наказуемых деяниях, как мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ), неправомерный доступ к компьютерной информации (ст. 272 УК РФ), создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ), преступления, совершаемые в сфере оборота цифровых активов (криптовалюты) (например, 205.1 УК РФ – содействие террористической деятельности путем ее финансирования) и т. п.

Подчеркнем, что вопрос классификации киберпреступлений носит практико-ориентированный характер, поскольку от этого зачастую зависит комплекс реализуемых превентивных мероприятий. Исследуя криминологическую характеристику отдельных составов киберпреступлений, следует отметить, что противодействие им осуществляется комплексно, в том числе с помощью оперативно-розыскных мероприятий, технических средств и отдельных специалистов в IT-сфере. Для этого и решается вопрос о классификации видов преступлений, составляющих цифровую преступность.

Перечислим группы преступлений рассматриваемой категории преступности.

---

[62] Ищук, Я. Г., Пинкевич, Т. В., Смольянинов, Е. С. Указ. соч. С. 80.

Первая группа цифровых преступных посягательств направлена на хищение имущества граждан и организаций (например, п. «г» ч. 3 ст. 158, ст. ст. 159.3, 159.6 УК РФ).

Вторая группа киберпреступлений – это общественно опасные деяния в сфере компьютерной информации. По данным ФКУ ГИАЦ МВД России, на 1 января 2022 года оставались нераскрытыми 10 229 преступлений, предусмотренных ст. 272 УК РФ, и 1 649 преступлений, предусмотренных ст. 273 УК РФ. Специальными подразделениями уголовного розыска, а также отделами «К» – бюро специальных технических мероприятий (далее по тексту – БСТМ) за январь – сентябрь 2022 года раскрыто:

а) 5 695 преступлений по ст. 272 УК РФ;

б) 172 преступления по ст. 273 УК РФ;

в) 518 преступлений по ст. 274.1 УК РФ[63].

Но часто преступления, указанные в данном перечне, являются лишь способом совершения других преступлений (например, мошенничеств).

Третья группа киберпреступлений связана с незаконным изготовлением и распространением порнографической продукции, материалов и предметов, в том числе с участием несовершеннолетних, посредством сети Интернет (например, ст. ст. 242, 242.1, 242.2 УК РФ).

Четвертая группа цифровых преступлений направлена на дистанционное распространение наркотических средств, психотропных и сильнодействующих или ядовитых веществ (например, ст. ст. 228.1, 234 УК РФ).

Согласно статистическим данным МВД России, за период 2017–2021 гг. прослеживается тенденция роста числа мошенничеств с применением ИТТ. Если в 2017 году количество таких преступлений составляло почти 81 000 случаев, то уже к концу 2021 года количество зарегистрированных подобных преступлений увеличилось почти в 4,4 раза. Для иллюстрации описываемой тенденции роста данной категории преступлений построим соответствующий график динамики официально зарегистрированных мошенничеств, совершенных с применением ИТТ (рис. 1).

[63] Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2022 года // Министерство внутренних дел Российской Федерации : офиц. сайт. URL: https://xn--b1aew.xn--p1ai/reports/item/35396677/ (дата обращения: 31.03.2023).

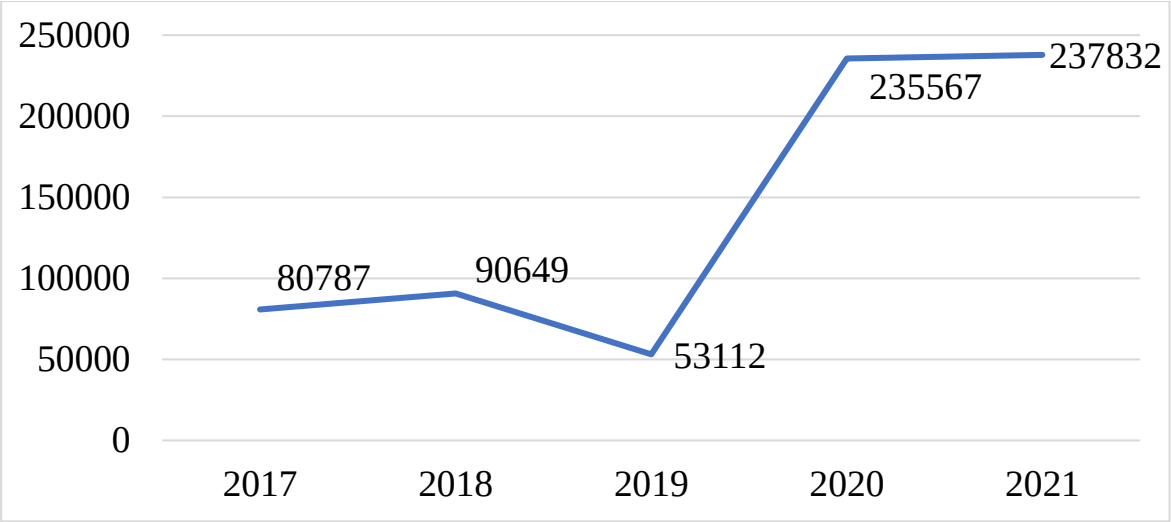

Рис. 1. Динамика преступлений, предусмотренных ст. 159 УК РФ (мошенничество), совершенных с применением ИТТ, за 2017–2021 гг.

Опираясь на данные представленного графика, можно сделать следующие выводы:

1. С 2018 г. по 2019 г. наблюдался спад количества выявляемых и регистрируемых мошенничеств с использованием ИТТ: почти в 2 раза – с 91 тысячи до 53 тысяч.

2. В период с 2019 г. по 2020 г. виден резкий статистический скачок регистрируемых показателей мошенничеств с применением ИТТ: с 53 тысяч до 236 тысяч. Увеличение показателя составило 4,4 раза, то есть 443,5 %. Вероятнее всего, статистический скачок указанного показателя явился результатом пандемии COVID-2019, когда был введен карантин и самоизоляция, люди были вынуждены использовать Интернет как средство заработка и жизнедеятельности.

Таким образом, в настоящей главе нами рассмотрены ключевые криминологические характеристики современной цифровой преступности. Далее обратимся к вопросу личности цифрового преступника.

ГЛАВА 5.
ЛИЧНОСТИ ЦИФРОВОГО ПРЕСТУПНИКА И ЕГО ЖЕРТВЫ

§ 1. Понятие и структура личностей цифрового преступника и его жертвы

Переходя к криминологическому портрету цифрового злоумышленника, дадим определение термину «личность преступника».

В науке криминологии под личностью преступника принято понимать совокупность социально-психологических свойств и качеств человека, являющихся причинами и условиями совершения преступлений[64].

По мнению Ю. М. Антоняна, личность преступника есть совокупность интегрированных в ней социально значимых негативных свойств, образовавшихся в процессе многообразных и систематических взаимодействий с другими людьми[65]. Также одним из главных отличий личности преступника от законопослушного гражданина является его духовность. Кроме того, исследования показывают, что процент импульсивности у преступника выше, чем у законопослушного гражданина. Импульсивность характеризуется слабой терпимостью и действием с агрессией при малейшем побуждении к этому. Стоит упомянуть, что именно такие индивиды применяют насилие различного рода при разрешении возникающих конфликтов.

В свою очередь, структура личности преступника – это криминологически упорядоченное соотношение свойств, характеризующих личность преступника [66].

Обозначим наиболее характерные признаки личности цифрового преступника (киберпреступника):

1) Высокий профессиональный уровень, поскольку для того, чтобы совершить подобное преступление, от преступника, как правило, требуется наличие специальных знаний, умений и навыков.

2) Наличие специального образования по направленности работы с ЭВМ или ИТТ.

---

[64] Степанова, М. А. Личность преступника: современные тенденции в криминологии // Вестник Нижегородской правовой академии : науч. журн. 2018. № 16 (16). С. 59.

[65] Цит. по: Коломытцев, Н. А., Одинцова, Л. Н. Личность преступника как криминологическая проблема // Государство и право: теория и практика : науч. журн. 2016. № 3 (4). С. 45.

[66] Сидорова, Е. З. Обеспечение криминологической безопасности в организациях общего и среднего профессионального образования : автореф. …канд. юрид. наук. Москва, 2018. С. 11.

3) Уверенность в своей безнаказанности. Поскольку в настоящее время киберпреступления характеризуются высоким уровнем латентности, многие злоумышленники решаются на их совершение в надежде остаться безнаказанными после их совершения.

4) Осознание того, что для совершения цифрового преступления не потребуется больших временных или материальных затрат (при условии наличия специальных познаний в цифровой сфере). Из-за своих особенностей киберпреступления требуют высокого профессионализма, однако при этом не требуют больших временных или материальных затрат, что влечет за собой завладение крупными денежными средствами, электронными средствами платежа, бездокументарными ценными бумагами или цифровой валютой по типу биткоина, догикоина и т. д.

При изучении личности цифрового преступника следует понимать, что цифровые преступления появились относительно недавно – в начале 90-х годов прошлого века. Это означает, что субъектами данных преступлений, как правило, выступают относительно молодые люди, которые начали интересовать ЭВМ и ИТТ по мере их распространения среди населения. Исходя из стереотипов, сложившихся в результате воздействия киноиндустрии, большинство «хакеров» представляются нам молодыми людьми, которые не нашли своего места в обществе, потому что не обладали (или считали, что не обладают) привлекательной внешностью или коммуникативными навыками. Такой молодой человек уходит в цифровой мир, где может быть тем, кем захочет, или же для осуществления своей мести в киберпространстве, например, для завладения персональными данными обидчика, что, несомненно, требует высокого профессионализма в сфере ЭВМ и ИТТ. Повышая свой профессионализм в информационной среде, преступник самоутверждается путем вознесения себя выше других индивидов в киберпространстве, где он обладает преимуществом в результате изучения компьютерных сетей и программирования, повышая свою самооценку как в собственных глазах, так и в глазах сверстников.

Анализ материалов судебно-следственной практики за 2012–2017 гг. позволил получить криминологически значимую информацию о личности компьютерного преступника в России. Типовой криминологический портрет российского компьютерного преступника в настоящее время выглядит следующим образом: мужчина возрастом до 35 лет, городской житель, имеющий среднее специальное или высшее техническое образование, не состоящий в браке (холост либо разведен), обладающий профессиональными навыками, имеющий опыт работы на компьютерных устройствах, специалист в области IT-технологий, либо безработный, который в силу своих профессиональных обязанностей имеет (имел) доступ к служебным компьютерным устройствам, компьютерным сетям и базам данных. Не имеет судимости и к уголовной ответственности

не привлекался, но в то же время компьютерные преступления совершал неоднократно. Преступные деяния предпочитает совершать в одиночку, так как обладает низкой социальной коммуникативностью и по характеру является индивидуалистом, эгоцентричной личностью[67].

Теперь обратимся к вопросу о характеристике тех лиц, которые, как правило, становятся жертвами цифровых преступлений. Потерпевший выступает одной из ключевых составляющих механизма самого преступления, поскольку именно потерпевший может мотивировать (осознанно или неосознанно) преступника совершить то или иное преступление.

Согласно толковому словарю С. И. Ожегова, под потерпевшим понимается человек, которому в результате преступления причинен моральный, физический или имущественный урон[68]. Понятие потерпевшего закреплено и в нормативных правовых актах, а именно в ч. 1 ст. 42 УПК РФ[69]. Согласно данной норме, потерпевшим является физическое лицо, которому преступлением причинен физический, имущественный, моральный вред. Однако существуют ситуации, когда само потерпевшее лицо не может представлять свои интересы в уголовном судопроизводстве. Такое возможно, например, при убийстве лица, и в таких случаях право потерпевшего представлять свои интересы в суде переходит к его близким родственникам или близким лицам.

Потерпевшего как участника преступления (или уголовного процесса, или судопроизводства) изучают такие научные отрасли, как криминология, уголовное право, уголовный процесс, а также профилирующая наука – виктимология (от лат. *victima* – «жертва» + др.-греч. λόγος – «учение»).

Сама виктимология зародилась относительно недавно, ее родоначальником считают американского криминолога Х. фон Хентинга, издавшего в 1948 году книгу «Преступник и его жертва». Стоит также упомянуть, что термин «виктимология» был использован в 1947 году психиатром Б. Мендельсоном[70].

Виктимология как обособленная теория криминологии изучает жертву, то есть характер и свойства поведения, а также ее роль и значение в совершенном преступлении. Личность индивида, ставшего жертвой

---

[67] Капинус, О. С. Криминология : учебник для вузов; 2-е изд., перераб. и доп. Москва : Юрайт, 2023. С. 249.

[68] Толковый словарь русского языка: 80000 слов и фразеол. выражений / С. И. Ожегов, Н. Ю. Шведова; 4-е изд., доп. М. : Азбуковник, 1997. С. 677.

[69] Уголовно-процессуальный кодекс Российской Федерации : УПК : принят Гос. Думой 22 ноября 2001 года : одобрен Советом Федерации 5 декабря 2001 года : послед. ред. // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_34481/ (дата обращения: 13.02.2023).

[70] Афанасьева, О. Р., Гончарова, М. В., Шиян, В. И. Указ. соч. С. 315.

преступления, характеризуется определенными чертами поведения при взаимодействии с преступником.

Одним из основополагающих терминов виктимологической науки является понятие «виктимизация», введенное в правовую литературу Л. В. Франком. Под виктимизацией он понимает процесс превращения лица в реальную жертву или конечный результат такого процесса. По его мнению, «виктимность определенного лица есть… не что иное, как реализованная преступным актом „предрасположенность“, вернее, способность стать при определенных обстоятельствах жертвой преступления, или, другими словами, неспособность избежать опасности там, где она объективно была предотвратима»[71].

Важно понимать, что потерпевший сам может вызывающе себя вести или быть идеальной жертвой для преступника, имея подходящее для преступника телосложение, характер и иные свойства личности. В таком случае возможно даже задаться вопросом, не отводить ли нам в таких ситуациях главенствующую роль в совершении преступления именно потерпевшему. Однако возможна и другая ситуация, когда жертва преступления не будет провоцировать преступника на совершение противоправного деяния, а лишь выступит частью совокупности детерминантов преступления.

Немалую роль в виктимности личности играют не только психофизиологические характеристики потенциальной жертвы, но и факультативные признаки объективной стороны преступления: место, время, обстановка и тому подобное, поскольку именно из-за совокупности всех этих факторов будет возможно совершение преступления.

Переходя к рассмотрению особенностей жертв цифровых преступлений, можно классифицировать типы указанных жертв по следующим основаниям:

1. В зависимости от состава цифрового преступления, в результате совершения которого данные лица стали жертвами.

2. В зависимости от демографических признаков, которые могли способствовать совершению в отношении них преступлений (пол, возраст, место работы и т. п.).

3. В зависимости от активности потерпевших. В этом случае можно выделить:

– активных потерпевших, поведение которых связано не с нападением на будущего преступника или конфликтным контактом с ним, а с активным способствованием причинению вреда самим себе

[71] Цит. по: Емельянов, И. Л. Виктимность и виктимизация: понятие, виды, проблемы профилактики // Известия Алтайского государственного университета : науч. журн. 2013. Т. 1. № 2 (78). С. 242.

(сознательные подстрекатели, неосторожные подстрекатели, сознательные самопричинители и неосторожные самопричинители)[72];

– пассивных потерпевших, не оказывающих сопротивления (не могущих или не хотящих это делать).

4. В зависимости от роли вины самих потерпевших в совершении преступления:

– антикриминогенная личность потерпевшего, противостоящая совершению преступления, т. е. лицо соблюдает личную безопасность и меры по предупреждению преступлений в отношении него (например, лицо не переходит по сомнительным интернет-ссылкам и не пользуется услугой самозаполнения окон на незнакомых сайтах, поскольку это могут быть фишинговые сайты; не распространяет персональные данные в сети Интернет и т. п.);

– криминогенная личность потерпевшего. В этом случае потерпевшее лицо, наоборот, побуждает и мотивирует преступника совершить преступление. Например, лицо загружает в общий интернет-доступ личные данные по определенному типу (номер банковской карты, паспортные данные и т. п.), чем злоумышленники могут воспользоваться и совершить киберпреступление;

– нейтральная личность потерпевшего. Потерпевший не способствует совершению преступления, но и не предпринимает никаких дополнительных мер безопасности в Интернете.

Говоря о криминологических особенностях жертв преступлений цифровой направленности, следует выделить их криминогенную роль в совершении противоправных деяний. Именно жертва может зародить у злоумышленника мотивацию совершения преступления своими личностно-волевыми характеристиками, умственными способностями, физическими особенностями, а также своей безынициативностью в вопросах обеспечения личной безопасности, в данном случае личной цифровой безопасности.

Своим поведением лицо может вызвать у субъекта преступления желание совершить определенный волевой акт, то есть зародить у злоумышленника некий импульс к совершению данного поступка, хотя последний знает, что данное деяние запрещено нормативными правовыми актами, а также общепринятыми нормами поведения в обществе, нормами морали и нравственности.

В виктимности жертв цифровых преступлений можно выделить две ключевые составляющие:

1. Возраст и пол потерпевшего. Чаще всего жертвами цифровых преступлений становятся люди, менее защищенные в цифровом

[72] Христенко, В. Е. Психология поведения жертвы : монография. Ростов н/Д : Феникс, 2004. С. 114.

пространстве. Как правило, это дети в возрасте 6–12 лет. Такие лица из-за особенностей возрастного и психологического характера еще не могут сами обеспечить безопасность своих интересов, в том числе в сети Интернет, и вместо них потерпевшими будут выступать их родители. Приведем гипотетический пример. Ребенок 10-ти лет, используя смартфон, переходит по ссылкам на различные интернет-сайты во время серфинга по Интернету (поясним, что серфинг в Интернете – это средство получения денег: пользователю платят деньги за просмотр или переход на конкретный веб-ресурс) и случайно заходит на фишинговый сайт или же становится жертвой спам-сообщений, где, например, говорится о том, что данный телефон был подвержен кибератаке и для сохранения всех данных необходимо с этого телефона отправить телефонный номер и номер банковской карты, в том числе с кодом с обратной стороны банковской карты, для успешного переноса данных из телефона в облачное хранилище. Ребенок в силу отсутствия опыта и психофизиологических особенностей своего возраста не способен идентифицировать данное деяние как преступление, в связи с чем подвергается собиранию у него персональной информации родителей. Подобная ситуация может произойти и со взрослыми людьми (как правило, речь идет о лицах в возрасте старше 50 лет). Приведем еще один пример. На телефон 60-тилетней женщины поступает звонок от якобы работника банка. Такой псевдоработник сообщает о срочной необходимости перевода всех денежных средств на другой лицевой счет, и сделать это нужно, по его словам, как можно скорее. Для этого мнимый сотрудник собирает у женщины необходимую информацию для перевода денежных средств с ее личного счета на счет преступника.

Приведем пример из правоприменительной практики.

Сорокалетняя жительница Курска дорого заплатила за урок, который ей преподали телефонные мошенники. С самого начала женщина продемонстрировала фантастическую доверчивость и поверила всему, что услышала в телефонной трубке. Человек, который представился сотрудником главного офиса банка, предложил курянке застраховать свои вклады от кражи. Никого не смутило, что вся процедура прошла дистанционно. Но затем собеседник заявил, что с одного из застрахованных счетов деньги уже были похищены, но страховка покроет ущерб. Взволнованную женщину заставили пойти в банк и закрыть свой счет на сумму более миллиона шестисот тысяч рублей. Ей объяснили, что это деньги, возмещенные по страховке, и их нужно вернуть, переведя через банкомат на несколько специальных счетов. И только потом с чеками о переводах прийти в отделение банка и получить свои деньги назад.

Курянке среди других позвонил и некий сотрудник следственных органов, который подтвердил, что расследует дело против неизвестных мошенников и убедил следовать инструкциям людей из банка и отправлять

наличность. Постепенно аферисты, желая сэкономить, перевели диалог в бесплатные мессенджеры. Потерпевшей стали рассказывать, что на ее имя пытаются оформить кредит злоумышленники. Чтобы этого не произошло, отправили в банк оформлять реальный заем. Все это время ситуация контролировалась дистанционно. Заявку на крупную сумму в офисе не приняли, предложив только кредитную карту с лимитом 150 тысяч рублей.

Телефонные аферисты заставили снять деньги и также перевести их, а когда поняли, что поживиться больше нечем, решили подшутить над жертвой. В мессенджере женщине прислали фото повестки от следователя. Она явилась в назначенный день в здание одной из силовых структур региона. Только там настоящие правоохранители открыли ей глаза на происходящее. Сейчас по факту мошеннических действий, совершенных неизвестными лицами, в УМВД России по г. Курску возбуждено уголовное дело. Злоумышленникам грозит наказание в виде лишения свободы на срок до 5 лет[73].

Несмотря на то, что жертвами кибермошенников может стать любой человек, существуют определенные группы риска. В первую очередь это люди старшего возраста, которые зачастую недостаточно хорошо разбираются в современных технологиях и которыми легче манипулировать. Так, по данным Центрального Банка России, на пожилых (60 лет и старше) приходится 27 % мошеннических действий, на возраст 50–59 лет – 20 %, 40–49 лет – 19 %, 30–39 лет –17 %, 20–29 лет – 13 %, младше 20 лет – только 4 %. Еще один интересный факт: оказалось, что женщины чаще, чем мужчины, попадаются на удочку мошенников – более 65 %[74].

Таким образом, следует констатировать, что возраст и пол потерпевшего относятся к одним из ключевых элементов виктимности граждан. Данные группы лиц имеют недостаточные знания работы с компьютерами и электронными сетями или имеют общий низкий или недостаточный уровень образования.

2. Значительный разрыв в осведомленности относительно работы ИТТ и ЭВМ злоумышленника и потенциальной жертвы. Данное положение объясняется тем, что рассматриваемый нами вид преступности зачастую требует высокого профессионализма в сфере ИТТ и ЭВМ. В противном случае субъект подобного преступления не сможет его совершить по причине отсутствия у него специальных знаний.

---

[73] Жительница Курска перевела мошенникам 1,7 миллиона рублей и пришла по подставной повестке в правоохранительные органы // Управление МВД России по Курской области : офиц. сайт. URL: https://46.xn--b1aew.xn--p1ai/news/item/33816305. Дата публикации: 17.11.2022.

[74] Горова, Н. 10 фактов о кибермошенничестве // +1 : сайт. URL: https://plus-one.ru/society/2021/06/30/10-faktov-o-kibermoshennichestve. Дата публикации: 30.06.2021.

Описанные нами признаки личности киберпреступника свидетельствуют о том, что работа с компьютерными сетями и ИТ-технологиями нередко является основным видом деятельности таких злоумышленников, в связи с чем цифровой преступник имеет значительное преимущество перед своей жертвой с точки зрения наличия у него специальных познаний в области цифровых технологий.

Виктимность жертв цифровых преступлений можно охарактеризовать как нейтральную и видовую. Нейтральной она является потому, что поведение жертвы не всегда обусловливает активизацию преступного поведения злоумышленника. Например, потенциальная жертва может получить сообщение в социальных сетях от знакомого человека, которого «взломали», т. е. жертва не осознавала и не была готова к тому, что от данного лица поступит фишинговое сообщение. Видовой же такая виктимность является потому, что все жертвы цифровых преступлений условно подходят под одни и те же критерии (низкая цифровая грамотность, низкий уровень бдительности, низкий уровень образования, высокая доверчивость), то есть речь идет о предрасположенности отдельных лиц при виктимогенной обстановке в совокупности с определенными обстоятельствами стать жертвой киберпреступления.

Как мы уже говорили, наиболее распространенным цифровым преступлением в настоящее время является кибермошенничество. В большинстве случаев при кибермошенничествах усматриваются признаки социальной инженерии. Чаще всего при совершении таких преступлений технические устройства работают исправно, защитные программы не подвергаются кибер-атаке, но преступление все же совершается. Объясняется это именно социальной инженерией, поскольку проще «взломать» человека с помощью психологических приемов, чем подвергать «взламыванию» то или иное техническое средство. Информационная безопасность включает в себя два аспекта: компьютер и человек. Компьютер взламывается с помощью специальных технических средств и вредоносного программного обеспечения, а человек – с помощью методов социальной инженерии. В данной совокупности наиболее уязвимым является именно человек, поскольку с развитием цифровой сферы растут протоколы безопасности, повышаются требования к антивирусным программам и создаются новые способы и методы защиты компьютерных сетей, а человек при этом не успевает меняться и по-прежнему остается мало защищенным от воздействия преступных методов социальной инженерии.

Впервые понятие «социальная инженерия» применил американский юрист, педагог, социолог права Роско Паунд. Кевин Митник (известный киберпреступник, позже консультант по компьютерной безопасности) в 1990-е гг. стал популяризировать данный термин. Он считал, что ни один

технический код не сможет так обмануть человека, как психологические умения преступника[75].

Социальная инженерия – это совокупность психологических, социологических методов и средств, направленных на создание благоприятных условий для выуживания, хищения засекреченных, конфиденциальных данных.

Для более детального понимания работы социальной инженерии приведем схему воздействия в социальной инженерии, составленную белорусским психологом и социологом В. П. Шейновым, долго занимавшимся психологией мошенничества (рис. 2)[76].

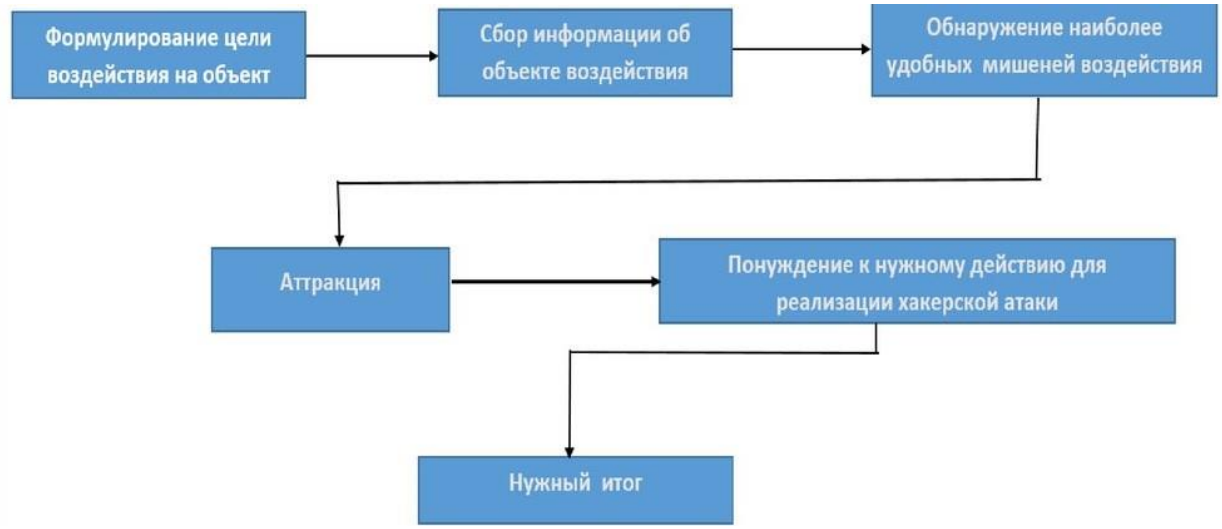

Рис. 2. Схема воздействия в социальной инженерии

Ярким примером применения методов социальной инженерии является мошенническая схема, которая была реализована в апреле 2020 года. В отдел полиции по району Замоскворечье обратилась 80-летняя жительница, которая сообщила, что на мобильный телефон ей поступил звонок и неизвестное лицо представилось местным участковым. Мужчина просил ее посодействовать в задержании группы мошенников, которая угрожает пожилым людям, вымогает у них вклады. Он попросил ее быть начеку. На следующий день пенсионерке позвонили с другого неизвестного номера, неизвестные мужчины начали ей угрожать и требовать снять ее деньги в банке. После данного звонка москвичка сразу вспомнила о звонившем ей «участковом» и решила позвонить ему для

[75] Янгаева, М. О. Социальная инженерия как способ совершения киберпреступлений // Вестник Сибирского юридического института МВД России : науч. журн. 2021. № 1 (42). С. 134.

[76] Кузнецов, М. В., Симдянов, И. В. Социальная инженерия и социальные хакеры : словарь. Санкт-Петербург : БХВ-Петербург, 2007. С. 112.

задержания злоумышленников. «Участковый», ответивший на звонок пенсионерки, сказал, что уже знает о них и они находятся в разработке для задержания. Затем попросил ее снять все деньги с банковского счета, выйти на балкон, сбросить деньги преступникам, чтобы их можно было задержать с поличным. Он сказал, что их задержат и деньги сразу вернут. Злоумышленники сразу подобрали пакет с деньгами и скрылись на автомобиле[77].

Согласно сравнительному исследованию, проводимому доктором психологических наук С. Ф. Сафуановым, для потерпевших в киберпространстве характерен следующий комплекс психологических особенностей: высокий уровень агрессии, низкая самооценка, неуверенность, апатия, вялость, нестабильное выражение эмоций, а также респонденты проводимого исследования были напряжены и раздражительны.

Внутри группы жертв противоправных посягательств в Интернете выделяются жертвы «насильственных» и «ненасильственных» преступлений, отличающиеся уровнем ситуативной и личностной тревожности, агрессивности и характером локуса контроля. Жертвы «насильственных» противоправных посягательств в Интернете более агрессивны, тревожны и относятся к экстернальному типу, в отличие от группы жертв «ненасильственного» типа, которые имеют более низкие показатели агрессивности, тревожности и относятся к интернальному типу[78].

Подводя итог, следует отметить следующее. Опираясь на ранее проводимые исследования, а также на анализ современных случаев совершения цифровых преступлений, мы предприняли попытку составить криминологические портреты классического цифрового преступника и его жертвы. Вместе с тем психологический портрет как цифрового преступника, так и его жертвы в настоящее время в научной литературе исследован недостаточно и нуждается, на наш взгляд, в более глубоком изучении, поскольку с развитием информационного общества меняются не только виды совершаемых цифровых преступлений, но и психологические характеристики жертв таких преступлений. В этой связи нам представляется необходимым проводить дальнейшие научные исследования по аналогичной тематике с целью формирования эффективных мер противодействия цифровой преступности в целом.

---

[77] Москвичка выбросила с балкона 6 миллионов рублей, чтобы помочь лжеучастковому задержать мошенников // Комсомольская правда : сайт. URL: https://www.kp.ru/daily/27118/4198857. Дата публикации: 15.04.2020.

[78] Сафуанов, Ф. С., Докучаева, Н. В. Особенности личности жертв противоправных посягательств в Интернете // Психология и право : электр. науч. журн. 2015. Т. 5. № 4. С. 89. URL: https://psyjournals.ru/journals/psylaw/archive/2015_n4/Safuanov_Dokuchaeva?ysclid=lru482e09a950732270 (дата обращения: 26.01.2024).

§ 2. Причины и условия преступности в сфере информационных (цифровых) технологий

Исследовав общую криминологическую картину цифровой преступности (на основе данных официальной статистики), обратим внимание на детерминацию (причины и условия) данного вида преступности. Углубленное изучение причин и условий цифровой преступности необходимо также для более полного определения криминологически значимых особенностей личностей цифрового преступника и его жертвы.

Причина всегда предшествует преступлению. Причина – необходимый источник следствия (преступности). Однако без необходимых условий она не существует и не может действовать[79].

Профессор А. И. Долгова говорит о том, что причинность равна следствию, но не может быть, чтобы следствие было равно причине, а также не может быть того, чтобы причина не предшествовала следствию. Но стоит также упомянуть, что без условий следствие просто не может существовать[80].

Под причинами преступности в криминологической науке понимаются некие обстоятельства, непосредственно обусловившие совершение преступления. В свою очередь, условия – это такие обстоятельства, которые способствовали совершению того или иного преступления, но прямо его не вызывали. При разграничении этих понятий следует отметить, что причины провоцируют преступность, а условия выступают только в качестве благоприятных обстоятельств. Взаимодействие данных факторов и их взаимное влияние друг на друга порождает в результате преступность.

Говоря об условиях преступности, отметим, что под данным термином понимается совокупность обстоятельств, при которых может возникнуть причина, а затем и само последствие. Важной составляющей самого преступного деяния является их неразрывная совокупность в преступном деянии, так как условие либо способствует возникновению причины, либо же создает такие явления, при которых сама причина может быть исполнена и совершено преступное деяние.

Кратко напомним, какие существуют в научной литературе подходы к вопросу о причинности преступности. Существует три ключевые концепции криминологической причинности: социальная, биологическая, психологическая. Они окончательно сформировались в 50–60-х годах прошлого века, когда отечественная криминология стала позиционировать себя в качестве самостоятельной, непосредственно обособленной научной

[79] Афанасьева, О. Р., Гончарова, М. В., Шиян, В. И. Указ. соч. С. 77.
[80] Долгова, А. И. Криминология : учебник. Москва : Норма, 2018. С. 91.

отрасли. Данные концепции объяснялись следующим образом: в основе биологической теории причинности преступности лежат заложенные природой (биологические) свойства и характеристики личности преступника; в основе психологической теории – субъективные детерминанты преступности; социальная концепция причинности преступности строилась на постулате об объективности процессов, лежащих в сфере социально-экономического устройства общества.

Если объяснять цифровую преступность, используя социальную теорию причинности, можно отметить, что в таком случае факторами преступности выступают имеющиеся социальные противоречия в обществе: экономические, политические, правовые организационные, психологические, технические, медицинские и т. д.

Правовой фактор заключается в несовершенстве законодательства. Например, Владимир Левин в 1994 году нанес крупный ущерб американскому банку Citibank, взломав его цифровое поле. Законодательство России на тот момент не предусматривало правовых норм, которые могли бы урегулировать данную ситуацию[81]. В подобных ситуациях и усматривается пробел в уголовно-правовой оценке общественно опасного деяния.

Экономический фактор выступает одной из причин преступности из-за наличия противоречий между потребностями и возможностями общества (например, расслоение общества по материальному положению).

Психологический фактор порождается нравственным кризисом в обществе и влечет за собой утрату общепринятых идеалов, доверия к правоохранительным органам, этническую и религиозную нетерпимость, алкоголизм, наркоманию, правовой нигилизм[82].

Следует также выделить некоторые ключевые детерминанты преступности:

– неблагоприятное влияние на личность в детстве и юности;

– низкий уровень материального благосостояния;

– низкий уровень культуры и моральных установок;

– воздействие на психику средств массовой информации;

– воздействие различных криминальных субкультур (например, криминальная культура скинхедов, движения А.У.Е);

– миграция населения (в таком случае люди находятся в более уязвимом состоянии и могут ради удовлетворения бытовых потребностей решиться на совершение противозаконного поступка).

Воздействие всех перечисленных детерминант на личность не будет являться основной причиной совершения преступления, потому что для его совершения необходимо волеизъявление самого субъекта, то есть

[81] Подстава века или таинственная история взлома Ситибанка // Хабр : сайт. URL: https://habr.com/ru/company/macloud/blog/552866/. Дата публикации: 19.04.2021.

[82] Капинус, О. С. Указ. соч. С. 124.

обстоятельства, влияющие на индивида, должны пройти через его сознание и волю. При одинаковом влиянии отрицательных обстоятельств отнюдь не каждый человек становится преступником, именно это и доказывает, что не только детерминанты составляют основу преступного поведения индивида, но и его внутреннее психическое отношение к совершаемому деянию.

Освещая детерминанты цифровой преступности, следует говорить о том, что человек, умышленно совершающий те или иные преступные действия, имеет специальные знания и умения для совершения своего преступного умысла. Особенно это характерно для цифровых преступников, поскольку для неправомерного доступа к компьютерной информации необходимо иметь навыки высокого профессионального уровня, которые не удастся получить в обычной общеобразовательной школе, из этого вытекает одно из условий цифровой преступности – высококвалифицированное образование в сфере ИТ-технологий.

Цифровая преступность требует высокого профессионализма, который обуславливается своевременным поглощением и усвоением информации в условиях быстрорастущей цифровизации, практическими навыками выполнения тех или иных задач, а также способностью к непрерывному обучению.

Рассмотрим данный тезис на примере такого знакомого многим людям Кевина Митника, о котором мы уже упоминали. Кевин начал свою карьеру с юных лет, а именно в 12 лет он уже мог спокойно перенаправлять звонки с таксофонов на домашний телефон, также умел звонить бесплатно. Затем в возрасте 16 лет он заинтересовался компьютерными сетями. Первым его крупным делом было то, которое нарушило законодательство США: Митник получил несанкционированный доступ к компьютерной сети компании Digital Equipment Corporation[83]. В конечном итоге Митник был осужден к реальному сроку отбывания наказания.

В подтверждение того, насколько важен для высокого профессионализма такой критерий, как постоянное обучение, отметим, что после своего освобождения Митник продолжил свою работу в сфере IT. Он создал компанию для решения вопросов компьютерной безопасности, однако сайт данной организации был подвержен ряду успешных кибератак, поскольку за время, проведенное им в тюрьме, произошло неизбежное развитие цифровых технологий, что и привело к тому, что Митник упустил те самые изменения в силу его объективной неспособности дальше развиваться в цифровом пространстве (в период отбывания наказания ему было запрещено пользоваться компьютером).

[83] Митник Кевин // Свободная энциклопедия «Википедия» : сайт. URL: https://ru.wikipedia.org/wiki/%D0%9C%D0%B8%D1%82%D0%BD%D0%B8%D0%BA,_%D0%9A%D0%B5%D0%B2%D0%B8%D0%BD (дата обращения: 28.08.2023).

Одной из причин, по которой злоумышленник все же решается на совершение преступного деяния, – это высокая латентность цифровых преступлений, потому что он наверняка знает, что останется безнаказанным за совершение преступления. Например, в 2019 году на территории Российской Федерации зарегистрировано 294 409 преступных посягательств, совершенных с применением ИТТ, из которых раскрыто только 65 238. Можно констатировать, что определенная часть преступлений в информационно-телекоммуникационном пространстве остается вне поля зрения правоохранительных органов[84].

Наибольшей латентностью обладают преступления, связанные с неправомерным доступом к охраняемой законом компьютерной информации. По мнению экспертов, латентность указанных противоправных посягательств составляет 80–85 %, а факты обнаружения незаконного доступа к информационным ресурсам на 90 % носят случайный характер[85].

Одной из детерминант цифровой преступности является то, что население в недостаточной степени информируется в призме киберпреступности о ее способах, методах и средствах, а также о лицах, ее совершающих, о том, каким образом они это делают, какие приемы используют.

Еще одним условием, провоцирующим совершение киберпреступлений, является низкая цифровая грамотность граждан различных стран, которая создает и ухудшает криминогенную обстановку в цифровой преступности. В общем спектре цифровую грамотность диктуют как совокупность навыков, знаний и умений для целесообразного использования всего спектра информационно-телекоммуникационных технологий. По мнению В. И. Токтарова и О. В. Ребко, под цифровой грамотностью следует понимать базовую компетенцию современного человека, которая включает в себя умения и навыки получения, оценки, обработки и производства информации с помощью цифровых технологий, выбор наиболее подходящих для реализации поставленных задач программно-технических средств, их безопасное использование, а также умение эффективно взаимодействовать с другими пользователями и решать коммуникативные задачи в условиях цифровой среды, используя для этого все ее сервисы и этические нормы[86]. К критериям цифровой грамотности следует отнести неисчерпывающий комплекс компонентов,

---

[84] Бойко, О. А., Унукович, А. С. Детерминанты латентных преступлений, совершаемых с использованием информационно-телекоммуникационных технологий // Юридический вестник Самарского университета : науч. журн. 2020. № 6 (3). С. 54.

[85] Там же. С. 55.

[86] Токтарова, В. И., Ребко, О. В. Цифровая грамотность: понятие, компоненты и оценка // Вестник Марийского государственного университета : науч. журн. 2021. Т. 15. № 2 (42). С. 168.

таких как разграничение искомой и необходимой информации от прочей, умение конкретно составить нужный запрос, навык определения идентичности информации искомой, знание такого явления, как «фейк», для его избежания, наличие основных знаний о цифровой безопасности, конфиденциальных данных и так далее.

Неотъемлемую часть цифровой грамотности составляет понятие информационной безопасности, которое изложено в Указе Президента Российской Федерации от 5 декабря 2016 года № 646. Информационная безопасность Российской Федерации – это состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства.

Из всего вышесказанного можно сделать вывод о том, что основными причинами преступности являются низкая духовность человека, чьи сознание и воля направлены на совершение аморальных действий, и низкий уровень его правового сознания. Таким образом, в качестве главной причины цифровой преступности можно рассматривать низкое духовное развитие человека, поскольку целью умышленных цифровых преступлений является, как правило, удовлетворение какого-либо корыстного интереса.

Подчеркнем, что раскрытие ключевых детерминант цифровой преступности будет способствовать выработке эффективной стратегии борьбы с киберпреступлениями, поскольку любое предупреждение строится в первую очередь на том, чтобы воздействовать на причины и условия преступности. В этой связи в следующей главе нашего пособия обратимся к вопросам и ключевым направлениям предупреждения цифровых преступлений.

ГЛАВА 6.
ПРЕДУПРЕЖДЕНИЕ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ (ЦИФРОВЫХ) ТЕХНОЛОГИЙ

§ 1. Понятие и основные направления предупреждения преступности в сфере информационных (цифровых) технологий

Информация – одна из важнейших составляющих в жизни, оказывающая влияние практически на все сферы жизнедеятельности человека. На сегодняшний день киберпреступность представляет большую угрозу современному миру, стремительно растет она и в России.

В этой связи обращение к вопросам профилактики и противодействия цифровой преступности является крайне актуальным и социально обусловленным.

Противодействие киберпреступности, а также различным преступным проявлениям, направленным на получение особо важной информации и преимущественно на хищение денег граждан и организаций, совершаемым при помощи ИТТ, относится к глобальным задачам, стоящим перед государством. Всплеск преступлений, совершаемых при помощи ИТТ, вызывает обеспокоенность среди правоохранительных органов (причем не только органов внутренних дел, но и органов прокуратуры и ФСБ России), а также в целом затрагивает национальные интересы Российской Федерации.

Поэтому предупреждение и раскрытие цифровых преступлений является неотъемлемой частью правоохранительной деятельности соответствующих субъектов профилактики. В частности, предупреждение, выявление, пресечение и раскрытие оперативными подразделениями органов внутренних дел преступлений в сфере компьютерной информации являются первоочередными задачами, решаемыми оперативно-розыскными органами полиции.

Под предупреждением цифровой преступности следует понимать деятельность различных субъектов профилактики, направленную на противодействие негативному воздействию, оказываемому на различные социальные блага цифровыми угрозами криминального характера.

Говоря о предупреждении цифровых преступлений, подчеркнем, что в нормативных правовых актах, в правоприменительной практике, в научной литературе можно встретить различные термины, отражающие направленность превентивной деятельности в данной сфере жизни социума: «направления предупреждения», «меры профилактики», «виды обеспечения предупредительной деятельности» и т. п. В конечном итоге речь идет о том, чтобы определить основные методы и приемы, которые

будут способствовать снижению негативного воздействия цифровых угроз криминального характера на различные социальные блага.

Как и превенция любого другого вида преступности, предупреждение цифровых преступлений предполагает осуществление целого ряда мероприятий, которые должны быть объединены единым целенаправленным замыслом по борьбе с данным видом преступлений. Иными словами, должна быть выработана единая государственная концепция (идея) по противодействию киберпреступности. Специалисты справедливо отмечают, что в реальной действительности предупреждение преступлений представляет собой сложную систему, состоящую из отдельных элементов деятельности разнообразного, многоуровневого характера, целью которой служит оказание воздействия на причины и условия, способствующие совершению преступлений, а также на лиц, их совершающих[87].

Основными направлениями предупреждения цифровых преступлений являются правовые, организационные, материально-технические, методические, кадровые и т. п.

Подчеркнем, что названные направления предупреждения цифровой преступности должны применяться вместе, в совокупности. При этом, несомненно, их реализация должна основываться на нормах действующего законодательства. В этой связи подчеркнем, что правовое регулирование предупреждения цифровых преступлений имеет первостепенное значение. Источниками правовых мер предупреждения цифровых преступлений традиционно являются уголовно-правовые нормы законодательства, устанавливающие ответственность за их совершение, а также нормы иных отраслей права, так или иначе затрагивающие вопросы предупреждения цифровых преступлений.

Однако, на наш взгляд, недостаточно только формально закрепить запрет на совершение того или иного цифрового преступления. Требуется выработать эффективный механизм реализации данных норм, что обеспечивается при помощи фактической реализации закрепленных превентивных мер борьбы с цифровой преступностью. Именно поэтому мы можем с уверенностью говорить о том, что нужен именно комплексный подход к реализации различных направлений предупреждения цифровой преступности.

На наш взгляд, помимо правовых мер превенции, большим профилактическим потенциалом обладают организационные меры борьбы с цифровыми преступлениями. К организационным мерам предупреждения цифровых преступлений можно отнести совокупность мероприятий, схематично изложенную ниже (рис. 3).

---

[87] Аносов, А. В. Специально-криминологическое предупреждение преступлений, совершаемых с использованием высоких технологий // Труды Академии управления МВД России : науч. журн. 2018. № 4 (48). С. 94.

Рис. 3. Организационные меры борьбы с цифровой преступностью

На наш взгляд, организационные меры борьбы с цифровой преступностью являются фундаментом, на котором строится вся система защиты компьютерной информации от неправомерного доступа.

В науке криминологии принято выделять несколько уровней предупреждения преступности: общесоциальный, специальный и индивидуальный. Каждый уровень превенции имеет значение для осуществления эффективного противодействия различным видам преступности. Не является исключением и предупреждение преступлений, совершаемых посредством цифровых технологий. Однако наибольшее внимание следует уделить специальному уровню предупреждения

обозначенного вида преступлений, поскольку именно данный вид превенции непосредственно направлен на причины и условия совершения преступлений.

Итак, говоря о специальном (специально-криминологическом) предупреждении уголовно наказуемых деяний, совершаемых посредством цифровых технологий, можно выделить следующие направления профилактики.

1) Повышение значимости научных исследований и теоретических разработок, посвященных вопросам борьбы с преступлениями, совершаемыми посредством цифровых технологий, для практической профилактической деятельности.

Отдельные специалисты придерживаются мнения о том, что снизить риски совершения тех или иных цифровых преступлений возможно только путем установления жестких запретов и контроля использования информационных (цифровых) технологий гражданами только в правомерных целях. Однако мы убеждены, что подобные запреты не только не решат проблему борьбы с цифровыми преступлениями, но и усугубят ее. Технический прогресс невозможно остановить ни правовыми запретами, ни жестким контролем со стороны правомочных лиц. Именно поэтому целесообразнее всего не бороться с научным прогрессом, а использовать его в целях борьбы с теми или иными преступлениями. В частности, в научной литературе можно встретить мнение, что необходима единая информационная база (система), позволяющая включить туда все доступные средства для борьбы с различными цифровыми преступлениями. Такая система позволила бы субъектам профилактики беспрепятственно обмениваться информацией, в том числе научными разработками и методиками, в процессе предупреждения, раскрытия и расследования цифровых преступлений[88].

2) Совершенствование правового регулирования сферы цифровых технологий.

В данном случае речь идет о том, что правотворчество всегда «запаздывает» с вопросом регулирования тех или иных общественных отношений. И это объективный процесс, поскольку социум и его отношения всегда развиваются быстрее. Законодатель только может «поспешить» с урегулированием уже сложившихся отношений.

Примером тому могут являться цифровые отношения, массовое развитие информационных и других компьютерных технологий, внедряемых во все сферы жизни современного человека. Многие государства не сразу отреагировали на изменение социальной реальности и на переход большого количества интересов граждан в виртуальную реальность.

[88] Там же. С. 95.

Например, в течение длительного периода отсутствовало правовое регулирование отношений, касающихся производства, купли-продажи и распространения криптовалюты. Государство предпринимало попытку не замечать развития данных отношений. Однако дальнейшее, не контролируемое государством, обращение криптовалюты стало невозможным, поскольку, пользуясь неурегулированностью отношений в сфере цифровой валюты, преступники стали использовать ее для совершения преступлений (мошенничества, взяточничество, финансирование терроризма, приобретение за счет криптовалюты наркотических средств и оружия и т. п.). В этой связи в России в 2020 году был принят Федеральный закон № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» (хотя рядом зарубежных стран уже давно были приняты подобные нормативные правовые акты). Более того, ряд государств уже давно предпринимает попытки контролировать цифровую сферу общественных отношений. Например, в Китае действует проект «Золотой щит» – это система фильтрации содержимого Интернета в КНР. Согласно общедоступной информации, разработка данного проекта была начата в 1998 году, а в 2003 году он был введен в эксплуатацию по всей стране. Этот проект включает систему управления безопасностью, систему информирования о правонарушениях, систему контроля выхода и ввода, информационную систему мониторинга, систему управления трафиком[89].

В настоящее время, несмотря на принятие Федерального закона о цифровой валюте, на практике по-прежнему не решено большое количество вопросов, связанных с теми или иными цифровыми правами. Например, исследователи задаются вопросом, возможно ли наследование криптовалюты, возможно ли ее включение или невключение в конкурсную массу должника (т. е. можно ли относить криптовалюту к имуществу должника, имеющемуся на дату открытия конкурсного производства и выявленного в ходе конкурсного производства) и т. д. И подобные вопросы не праздные. Они продиктованы реально складывающимися общественными отношениями, которые требуют своего правового регулирования.

Проблема усугубляется тем, что в настоящее время отсутствует нормативно закрепленное определение термина «цифровые преступления». Как мы уже говорили, в научной литературе можно встретить различные термины, отражающие понятие «цифровая преступность». И такое многообразие стало возможным именно ввиду отсутствия законодательно закрепленного понятия, что именно следует

[89] Золотой щит // Свободная энциклопедия «Википедия» : сайт. URL: https://ru.wikipedia.org/wiki/%D0%97%D0%BE%D0%BB%D0%BE%D1%82%D0%BE%D0%B9_%D1%89%D0%B8%D1%82#cite_note-1 (дата обращения: 28.08.2023).

понимать под цифровыми преступлениями и какие составы преступлений следует относить к их числу.

Особенностью цифровой преступности является то, что те составы преступлений, которые можно признать цифровыми, не объединены в единую главу, они разрозненно расположены в УК РФ. Кроме того, цифровым преступлениям не уделяется достаточного профилактического внимания (в силу как объективных, так и субъективных причин), что является ошибочной практикой, поскольку цифровая преступность на данный момент только развивается, а преступники находят все более изощренные методы и способы совершения цифровых преступлений.

По нашему мнению, превенция киберпреступлений должна строиться на разрешении вопросов унификации и легитимизации терминов и определений в области цифровых технологий.

3) Совершенствование механизма взаимодействия субъектов профилактики и предупреждения преступлений, связанных с финансированием экстремистской деятельности и терроризма, совершаемых посредством цифровых технологий.

Данная мера является значимой для практической деятельности, поскольку именно от слаженности действий всех субъектов профилактики зависит эффективность превенции в целом. По верному замечанию исследователей, несогласованность субъектов предупреждения преступлений в той или иной сфере зачастую предоставляет дополнительные возможности для преступных комбинаций[90]. Именно поэтому предупредительные меры будут иметь практический эффект только тогда, когда будет осуществляться взаимодействие государственных и муниципальных органов власти с институтами гражданского общества, в том числе общественными объединениями, средствами массовой информации, образовательными и научными организациями и т. д.

4) Законодательная регламентация вопросов, связанных с обеспечением информационной безопасности в обществе. Речь идет о необходимости законодательного закрепления следующих положений[91]:

– обязанности производителей и продавцов компьютерной техники и средств связи устанавливать в свою продукцию антивирусные продукты в целях защиты от несанкционированного доступа к компьютерной информации;

– системы страхования информационных рисков. Речь идет о необходимости и целесообразности страхования средств передачи, обработки или хранения охраняемой компьютерной информации, информационно-телекоммуникационных сетей и оборудования

[90] Аносов, А. В. Указ. соч. С. 94.
[91] Там же. С. 96.

от неправомерного блокирования, уничтожения, модификации либо несанкционированного копирования электронной информации;

– обязанности для физических лиц указывать свои персональные данные при регистрации сайтов, веб-страничек, получении аккаунтов в социальных сетях и т. п. (указывать свои ФИО, год рождения, данные паспорта). При этом речь идет не о том, что данная информация должна в обязательном порядке стать открытой и доступной для окружающих, а о том, что данная информация необходима именно для регистрации в интернет-пространстве;

– различных нормативных предписаний, направленных на своевременное реагирование правовой базы на изменяющиеся условия функционирования систем защиты информации и информационных ресурсов. Примером такого своевременного правового реагирования может служить действующий на территории Китая проект «Золотой щит» – система фильтрации содержимого Интернета в КНР, о которой мы уже упоминали;

– полномочий правоохранительных органов на осуществление мониторинга опубликованных в сети Интернет материалов противоправного характера. Специалисты отмечают, что в настоящее время назрела необходимость предоставить правоохранительным органам возможность проводить соответствующие надзорные, оперативно-розыскные, следственные мероприятия для получения необходимой информации от провайдеров или Роскомнадзора напрямую без судебного разрешения[92].

5) Совершенствование практической деятельности субъектов, деятельность которых направлена на противодействие киберпреступности. В данном случае можно говорить о следующих направлениях превенции:

– совершенствование актуальных прикладных методик противодействия цифровой преступности;

– совершенствование системы подготовки сотрудников как правоохранительных органов, так и частных компаний в области информационной, цифровой безопасности, что позволит готовить и выпускать высококвалифицированных специалистов в данной области[93];

– совершенствование порядка реализации мероприятий по обмену опытом, проведения на регулярной основе курсов повышения квалификации, стажировок в практических органах, семинаров и круглых столов для сотрудников и профессорско-преподавательского состава ВУЗов в образовательных организациях, а также в компаниях,

[92] Там же. С. 96.

[93] Шевко, Н. Р. Проблемы подготовки специалистов по раскрытию и расследованию преступлений, совершенных с использованием современных информационных технологий, в образовательных организациях МВД России // Вестник Казанского юридического института МВД России : науч. журн. 2017. № 1 (27). С. 89.

занимающихся цифровой безопасностью. В частности, подобная деятельность осуществляется на базе IT-компании «Лаборатория Касперского», а также на базе международного учебно-методического центра финансового мониторинга (МУМЦФМ), одна из целей деятельности которого заключается в организации и проведении учебно-методических мероприятий по вопросу противодействия цифровому финансированию терроризма, в том числе путем реализации образовательных программ дополнительного профессионального образования;

– отказ от территориальной подследственности в вопросах расследования цифровых преступлений. Одной из главных особенностей всех цифровых преступлений является ее трансграничный и зачастую многоэпизодный характер. В этой связи на практике часто возникают сложности с определением места совершения преступления, а значит, присутствуют сложности с определением конкретного органа, который должен заниматься его расследованием на основании принципа территориальной подследственности. Поскольку в виртуальном мире понятие территориальности трудноопределимо, целесообразней отказаться в расследовании таких дел от принципа территориальной подследственности и избрать принцип функциональности. Иными словами, в раскрытии и расследовании таких преступлений целесообразно следовать специализации сотрудников оперативных и следственных подразделений;

– совершенствование информационно-аналитического обеспечения деятельности по борьбе с цифровыми преступлениями. В частности, речь идет о необходимости более широкого внедрения достижений науки в работу правоохранительных органов, связанную с противодействием цифровым преступлениям. Специалисты приводят пример, когда на базе УМВД России по Мурманской области была разработана и апробирована информационно-поисковая система «Дистанционное мошенничество». Данная система во многом облегчает работу специальных субъектов, занимающихся борьбой с цифровыми мошенничествами[94];

– совершенствование взаимодействия правоохранительных органов со средствами массовой информации (далее – СМИ). По верному замечанию специалистов, для того чтобы деятельности СМИ способствовала борьбе с цифровыми преступлениями, в том числе борьбе с финансированием экстремизма и терроризма, осуществляемым посредством цифровых технологий, необходимо, чтобы представители СМИ[95]:

---

[94] Опальский, А. П., Смирнов, А. И. О деятельности информационно-поисковой системы по противодействию дистанционному мошенничеству // Алтайский юридический вестник : науч. журн. 2017. № 3 (19). С. 48.

[95] Аносов, А. В. Указ. соч. С. 97.

– транслировали своим читателям и зрителям отчеты правоохранительных органов перед населением о результатах борьбы с данными преступлениями;

– осуществляли правовую пропаганду, направленную на формирование правосознания и нетерпимости к преступным проявлениям;

– информировали население о средствах и методах защиты от цифровых преступлений, о новых формах и схемах их осуществления.

Подчеркнем, что различные меры предупреждения цифровых преступлений всегда реализуются теми или иными субъектами, отдельными лицами. В следующем параграфе раскроем вопрос о таких субъектах.

§ 2. Субъекты предупреждения преступности в сфере информационных (цифровых) технологий

В научной литературе отмечается, что в зависимости от предназначения субъектов предупреждения и от того, для чего данные субъекты были созданы и функционируют, они подразделяются на специализированные и неспециализированные[96].

1. Специализированные органы, основной целью которых является обеспечение цифровой безопасности в государстве. К данной категории субъектов следует отнести:

– ФСБ России;

– Службу внешней разведки Российской Федерации;

– Министерство обороны Российской Федерации;

– Росгвардию;

– МВД России;

– ФСО России.

2. Неспециализированные государственные и общественные органы, организации и объединения, занимающиеся превентивной работой наравне с иной деятельностью (предупреждение цифровой преступности не является основным видом деятельности):

– органы государственной власти Российской Федерации и органы местного самоуправления, осуществляющие управление в различных сферах жизнедеятельности общества;

– образовательные организации;

– институт семьи, родители, близкие родственники;

– средства массовой информации;

[96] Цит. по: Сидорова, Е. З., Грибунов, О. П. Предупреждение преступлений и административных правонарушений органами внутренних дел : учеб. пособие. Иркутск, 2023. С. 14.

– отдельные граждане и в целом общество, поскольку в той или иной мере каждый гражданин задействован в предупреждении цифровой преступности.

Поскольку цифровые технологии стали широко применяться в повседневной жизни, очень важно осуществлять комплексное взаимодействие различных субъектов профилактики (как специализированных, так и неспециализированных) между собой. Говоря о субъектах, оказывающих противодействие преступной деятельности, осуществляемой посредством цифровых технологий, следует обратить внимание на криптовалютную биржу Binance. В 2022 году данная биржа запустила систему помощи государственным регуляторам и правоохранительным органам под названием Law Enforcement Request System (LERS)[97]. Суть данного решения заключается в том, что представители власти смогут отправлять на платформу запросы для предоставления информации о пользователях, необходимой в рамках уголовных расследований. Каждая заявка рассматривается в индивидуальном порядке с учетом пользовательского соглашения и применяемого законодательства. Иными словами, в рамках уголовных дел сотрудники биржи Binance решили предоставлять информацию о своих пользователях и совершаемых ими транзакциях. Данное положение будет подрывать принцип анонимности проводимых на бирже Binance операций с криптовалютой, а значит, будет способствовать борьбе с цифровыми преступлениями.

В профилактике киберпреступности большая роль отводится частным (негосударственным) структурам. Например, на базе IT-компании «Лаборатория Касперского», а также в компаниях, занимающихся цифровой безопасностью, большое внимание уделяется вопросам обучения сотрудников навыкам обеспечения цифровой безопасности. Подобная деятельность осуществляется и в государственном секторе, например на базе международного учебно-методического центра финансового мониторинга (МУМЦФМ).

Особое внимание следует уделить специализированным субъектам профилактики цифровых преступлений.

Так, контроль за соблюдением требований к защите информации и эксплуатации специальных программно-технических средств защиты информационных систем, обрабатывающих информацию с ограниченным доступом в негосударственных структурах, осуществляется органами государственной власти.

Правительство Российской Федерации определяет порядок осуществления такого контроля. В организациях, обрабатывающих

[97] Система запросов для правоохранительных органов // Binance : сайт. URL: https://www.binance.com/ru-UA/support/law-enforcement (дата обращения: 10.09.2023). Режим доступа: для зарегистрир. пользователей.

государственную информацию с ограниченным доступом, создаются специальные службы, обеспечивающие защиту такой информации.

Собственник информационных ресурсов или уполномоченные им лица имеют право осуществлять контроль за выполнением требований по защите информации и запрещать или приостанавливать обработку информации в случае невыполнения этих требований.

Практика борьбы с цифровыми преступлениями показывает, что положительный результат можно получить только при использовании комплекса правовых, организационных и технических мер предупреждения цифровых преступлений, причем все они одинаково важны и, лишь дополняя друг друга, образуют целенаправленную систему предупреждения и профилактики исследуемого вида преступности, а обеспечить системную реализацию всех мер превенции могут только все субъекты вместе. В вопросах борьбы с цифровыми преступлениями субъекты профилактики должны действовать сообща и выстраивать эффективный механизм взаимодействия и обмена необходимой информацией.

Подчеркнем, что особое место в системе субъектов, осуществляющих деятельность по предупреждению цифровых преступлений, занимают органы внутренних дел, в частности Управление по организации борьбы с противоправным использованием ИТТ.

Противодействие рассматриваемым преступлениям включает в себя полный комплекс мер оперативно-технических, поисковых, оперативно-розыскных действий, в том числе разъяснительные и профилактические средства общей и индивидуальной профилактики правонарушений, которые предусмотрены действующим законодательством.

Следует отметить, что оперативные подразделения полиции, в зависимости от их компетенции, выполняя свое законодательное предназначение, задействованы в реализации приоритетных направлений деятельности полиции, таких как предупреждение, пресечение, выявление и раскрытие преступлений, в том числе совершаемых с использованием информационно-коммуникационных технологий.

Основными субъектами, осуществляющими выявление, предупреждение, пресечение и раскрытие преступлений, розыск лиц, совершивших преступления при помощи ИТТ, а также в дальнейшем оперативное сопровождение уголовных дел на стадии предварительного расследования, являются сотрудники специализированных подразделений уголовного розыска, а также БСТМ[98].

Важно отметить, что только слаженная деятельность различных органов по предупреждению рассматриваемой категории преступлений

[98] Осипенко, А. Л. Об участии органов внутренних дел в системе обеспечения кибербезопасности Российской Федерации // Общество и право : науч. журн. 2018. № 3 (65). С. 43.

способна минимизировать их последствия, в первую очередь – в виде хищений денежных средств и утечки информации. Эффективность борьбы с киберпреступлениями часто зависит от качественного и слаженного взаимодействия не только между различными структурными подразделениями органов внутренних дел, но и с иными органами, осуществляющими противодействие преступности. В этой связи сотрудники органов внутренних дел, а также обучающиеся, готовые стать действующими сотрудниками правоохранительной системы, должны понимать, что основа эффективной борьбы в данном случае заключается в умении выполнять свои функции совместно с другими субъектами профилактики, умении взаимодействовать друг с другом.

§ 3. Основные меры предупреждения преступности в сфере информационных (цифровых) технологий

Прежде чем раскрыть ключевые меры предупреждения цифровой преступности, отметим, что в научной литературе выделяются различные основания классификации данных мер[99].

В частности, если брать за основу такой критерий, как характер реализуемых мер, можно выделить:

1) процессуальные и внепроцессуальные меры;

2) запрещающие меры, ограничивающие меры, обязывающие меры.

Взяв за основу критерий масштабности мер, можно выделить:

1) общегосударственные меры;

2) региональные меры;

3) местные меры, реализуемые на уровне муниципального образования;

4) локальные меры, осуществляемые конкретной организацией или иным лицом.

Как мы уже говорили, в основе предупреждения цифровых преступлений лежит нормативное регулирование отношений в сфере цифровых технологий. Следует обозначить предписания таких нормативных правовых актов, как:

– Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

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

---

[99] Чепрасова, Ю. В., Шмарион, П. В. Основные направления противодействия киберпреступности // Вестник Воронежского института МВД России : науч. журн. 2020. № 3. С. 257.

– Указ Президента Российской Федерации от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации»[100].

При этом важное практическое значение имеет организация контроля за исполнением положений названных нормативных правовых актов, поскольку ключевое значение имеет не только закрепление какого-либо правила в том или ином правовом акте, но и установление механизма его реализации, в том числе путем определения механизма контроля за его исполнением. Контроль осуществляют субъекты, которые наделены соответствующими полномочиями и являются ответственными за исполнение данного полномочия.

В основе современного механизма предупреждения цифровых преступлений лежит также институт информационно-аналитического обеспечения такого предупреждения, правовая основа которого закреплена в ст. 31 Федерального закона от 23 июня 2016 года № 182-ФЗ «Об основах системы профилактики правонарушений в Российской Федерации»[101]. Согласно данной норме, в целях информационного обеспечения профилактики правонарушений субъекты профилактики могут использовать в своей деятельности информационные ресурсы СМИ, сети Интернет и т. д., размещая в цифровом пространстве необходимую информацию.

Однако институт информационно-аналитического обеспечения предупреждения цифровой преступности не ограничивается только использованием СМИ и сети Интернет. Информационно-аналитическое обеспечение предполагает также использование различных информационных банков данных, различного программного обеспечения, направленного на своевременное получение оперативно значимой информации, необходимой для успешного предупреждения и пресечения совершаемых цифровых преступлений. В этом и заключается первостепенная цель информационно-аналитического обеспечения предупреждения цифровых преступлений. При этом подчеркнем, что существуют различные базы данных, которые могут и не быть напрямую связаны с совершаемым цифровым преступлением, но могут помочь выявить лицо, совершающее данное преступление. Например, существуют

---

[100] О развитии искусственного интеллекта в Российской Федерации : Указ Президента Российской Федерации от 10 октября 2019 года № 490 // Официальный интернет-портал правовой информации : сайт. URL: http://publication.pravo.gov.ru/Document/View/0001201910110003?index=1 (дата обращения: 20.03.2023).

[101] Об основах системы профилактики правонарушений в Российской Федерации : Федер. закон № 182-ФЗ : принят Гос. Думой 10 июня 2016 года : одобрен Советом Федерации 16 июня 2016 года // Кодекс: Электронный фонд правовых и нормативно-технических документов : сайт. URL: https://docs.cntd.ru/document/420361608 (дата обращения: 21.03.2023).

такие банки данных, как Единый реестр нарушителей правил дорожного движения, Паспорт наркотического контроля, Федеральный реестр населения, База данных о паспортных данных граждан Российской Федерации, Ведомость недействительных паспортов, Банк данных о судимости лиц, Банки данных о лицах, находящихся в розыске, и многое другое.

Отдельно можно также обозначить программно-технический комплекс (далее – ПТК) «Интегрированный банк данных – Регион» (далее – ИБД-Р). В ИБД-Р интегрируются все оперативно-справочные, криминалистические и розыскные учеты ОВД. ИБД-Р реализуется на основе системы управления базами данных (СУБД) Oracle. Для удаленного доступа используются система S4Clone. Вся информация представлена в виде документов, а именно справок и первичных документов. ИБД-Р объединяет в себе специализированные автоматизированные информационно-поисковые системы (АИПС), оперативно-справочные учеты и единую систему учетов преступлений. За пределами ИБД-Р остаются дактилоскопическая система на базе «Папилон» и системы статистического учета[102].

Необходимыми элементами аналитической работы являются прогнозирование и планирование борьбы с преступностью. Несомненно, использование современного информационно-аналитического обеспечения необходимо и объективно обусловлено в целях пресечения совершаемого или совершенного цифрового преступления. Однако долгосрочное предупреждение ориентировано на то, чтобы подобные преступления не совершались вовсе. А для этого важно осуществлять соответствующее криминологическое прогнозирование.

Криминологическое прогнозирование – это предсказание будущего состояния преступности и связанных с ней явлений, а также выявление основных тенденций их развития.

В зависимости от охватываемых временных этапов криминологическое прогнозирование подразделяется на следующие виды:

1) краткосрочное криминологическое прогнозирование (прогноз составляется на срок от 1 месяца до 1 года);

2) среднесрочное криминологическое прогнозирование (дается прогноз сроком до 5 лет);

3) долгосрочное криминологическое прогнозирование (как правило, срок прогноза составляет от 5 до 15 лет)[103].

---

[102] Мачтаков, С. Г., Питолин, М. В., Мальцев, С. А. Использование возможностей специализированных банков данных МВД России в раскрытии и расследовании преступлений // Пожарная безопасность: проблемы и перспективы : науч. журн.. 2015. Т. 2. № 1 (6). С. 374.

[103] Сидорова, Е. З. Примерный прогноз развития криминальной ситуации на объектах транспортной инфраструктуры Восточно-Сибирской железной дороги // Социально-экономический и гуманитарный журнал : науч. журн. 2022. № 3 (25). С. 156.

Объектом криминологического прогнозирования выступают преступность, личность преступника, детерминанты преступности, ее последствия и меры борьбы с преступностью.

В свою очередь, предметом криминологического прогнозирования являются состояние, тенденции, периоды развития конкретного объекта криминологического прогнозирования.

Подчеркнем, что в эпоху цифровизации общества возможности для составления наиболее точного криминологического прогноза обширны. В частности, одним из методов составления криминологического прогноза является метод математического моделирования, в основу которого кладутся различные показатели, влияющие на показатели преступности. Благодаря специальной компьютерной программе данные факторы сводятся воедино, и данная программа выстраивает примерный прогноз преступности. Однако следует учитывать, что криминологический прогноз носит вероятностный характер и не всегда сбывается в полном объеме.

Помимо вышесказанного важно также отметить, что в основе борьбы с цифровыми преступлениями должна лежать комплексная программа противодействия цифровой преступности. В настоящее время на территории нашей страны действует государственная программа по противодействию преступности[104]. Однако данная программа не учитывает особенности современной цифровой преступности, в связи с чем, на наш взгляд, требует пересмотра и доработки.

Пресечение и раскрытие киберпреступлений обязано идти в ногу со временем, и порой старые способы и средства проведения превентивных мероприятий носят лишь вспомогательный характер. Эффективная борьба с киберпреступностью невозможна без применения новых технологий, способов и средств осуществления профилактики.

Подчеркнем, что предупреждение цифровых преступлений невозможно без проведения различных оперативно-розыскных мероприятий. Как справедливо отметили А. И. Розенцвайг и В. С. Чертилин, «необходимость модернизации превентивных мер вызвана уникальностью сетевого пространства и специфики совершаемых в нем преступлений, характеризующихся удаленностью, динамичностью и выходом за пределы одного государства»[105].

---

[104] Об утверждении государственной программы Российской Федерации «Обеспечение общественного порядка и противодействие преступности» : Постановление Правительства Российской Федерации от 15 апреля 2014 года № 345 : послед. ред. // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_162172/e2f7a237e73e3fa254c97c38364a9a392a8a32ef/?ysclid=lmd7h6smv2837605191 (дата обращения: 20.03.2023). Режим доступа: для зарегистрир. пользователей.

[105] Розенцвайг, А. И., Чертилин, В. С. Формы противодействия киберпреступности // Вестник экономики, права и социологии : науч. журн. 2019. № 4. С. 13.

Согласно приказу МВД России от 19 июня 2012 г. № 608 «О некоторых вопросах организации оперативно-розыскной деятельности в системе МВД России»[106], подразделения уголовного розыска и БСТМ вправе осуществлять оперативно-розыскную деятельность в полном объеме, предусмотренном Федеральным законом от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности»[107] (далее – ФЗ «Об ОРД»).

В этой связи сотрудники данных подразделений, занимаясь пресечением и раскрытием киберпреступлений, реализуют правоохранительную функцию государства. Важно отметить, что необходимость иметь в распоряжении оперативных подразделений органов внутренних дел комплекс негласных оперативно-розыскных мероприятий и технических средств объясняется тем, что раскрыть данные преступления при помощи одних только следственных действий и гласных мер административного характера практически невозможно.

В практической деятельности оперативных подразделений для пресечения и раскрытия преступлений рассматриваемой категорий наиболее применимы оперативно-технический, агентурный и следственный (уголовно-процессуальный) методы, а также отдельные оперативно-розыскные мероприятия, применяемые по мере необходимости и в зависимости от имеющейся оперативно значимой информации. Рассмотрим их более подробно.

Оперативно-технический метод. Суть данного метода заключается в осуществлении оперативно-розыскной деятельности путем применения сотрудниками оперативных подразделений в негласной форме следующих оперативно-розыскных мероприятий, предусмотренных ст. 6 ФЗ «Об ОРД»: прослушивание телефонных переговоров; снятие информации с технических каналов связи; получение компьютерной информации.

Указанный метод также включает в себя применение мониторинга и системного анализа информации, размещенной в цифровой среде сети Интернет, который охватывает также неиндексируемый сегмент в поисковых системах (например, Darknet, Dark Web, Deepnet, Deep Web). В сочетании с аналитикой больших данных метод позволяет формировать целостную картину интернет-пространства в целях выявления потенциальных и реальных угроз их более оперативного обнаружения и реагирования.

---

[106] О некоторых вопросах организации оперативно-розыскной деятельности в системе МВД России : приказ МВД России от 19.06.2012 № 608 : послед. ред. // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_133312/ (дата обращения: 20.03.2023). Режим доступа: для зарегистрир. пользователей.

[107] Об оперативно-розыскной деятельности : Федер. закон № 144-ФЗ : принят Гос. Думой 5 июля 1995 года : послед. ред. // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_7519/ (дата обращения: 20.03.2023).

В соответствии с ч. 1 ст. 14 ФЗ «Об ОРД», при решении задач, связанных с пресечением и раскрытием преступлений рассматриваемой категории, у сотрудников оперативных подразделений в процессе проведения ОРМ возникает обязанность защищать законные интересы пострадавших от преступлений, совершаемых с использованием ИТТ.

Специфика пресечения и раскрытия киберпреступлений связана с реальным ограничением прав широкого круга лиц на тайну переписки, телефонных переговоров и иных сообщений, передаваемых по сетям электрической связи, а также ограничением их права на банковскую тайну.

Как правило, к таким лицам относятся как непосредственно фигуранты, в отношении которых имеются сведения об их причастности к совершенным преступлениям, так и различные подставные или сопутствующие лица (владельцы различных гаджетов; владельцы интернет-кафе; номинальные директора коммерческих организаций; обладатели СИМ-карт; лица, обналичивающие денежные средства, и т. п.).

Важно отметить, что ограничение конституционных гарантий граждан допустимо на основании судебного решения и, соответственно, требует соблюдения процедур, регламентированных законами, подзаконными правовыми актами, локальными актами коммерческих организаций, а при проведении негласных мероприятий – и особого порядка секретного делопроизводства.

Агентурный метод. Данный метод также актуален в современных условиях для пресечения и раскрытия киберпреступлений, так как, несмотря на дистанционный характер, их все-таки совершают люди, которые имеют определенные социальные связи и круг общения. Однако данные люди ведут, как правило, закрытый, конспиративный образ жизни и имеют высокий уровень анонимности за счет использования технологий шифрования.

Названный метод представляет собой определенную совокупность способов и приемов легендированного поведения негласных сотрудников (агентов), а также действующих сотрудников оперативных подразделений по получению (выведыванию) оперативно значимой информации и в дальнейшем документированию преступной деятельности путем установления или развития доверительных отношений с обладателями такой информации.

Сотрудники оперативных подразделений продолжают использовать наиболее доступные и отработанные годами оперативно-розыскные мероприятия, такие как наблюдение, опрос, оперативное внедрение в среду специалистов в сфере ИТТ. Они изучают культуру хакеров, работают с лицами, осужденными за компьютерные преступления, с их кругом общения.

Следует отметить, что одним из источников информации, получаемой оперативным путем, является наблюдение за IT-специалистами, попавшими в поле зрения правоохранительных органов, а также сотрудничество с ними на конфиденциальной основе. Одним из видов ОРМ является наблюдение за местами сетевого общения хакерского сообщества, где осуществляется обмен криминальным опытом, а также информацией о жертвах и способах совершения общественно опасных деяний. Наблюдение и опрос осуществляется самими сотрудниками полиции, а также происходит посредством работы с конфидентами, которые имеют отношение к рассматриваемой преступной среде[108].

В случае получения реальной информации о готовящемся либо совершенном преступлении подключается техническая составляющая оперативно-розыскной деятельности и проводятся иные необходимые оперативно-розыскные мероприятия. В частности, при проведении ОРМ «наведение справок» по учетам операторов связи, кредитно-финансовых организаций, виртуальных торговых площадок и иных онлайн-сервисов в целях пресечения и раскрытия преступлений оперативные подразделения требуют от них предоставить сведения, составляющие коммерческую тайну.

При раскрытии преступлений, связанных с неправомерным доступом к компьютерной информации (ст. 272 УК РФ), созданием, использованием и распространением вредоносных компьютерных программ (ст. 273 УК РФ), работа по раскрытию сконцентрирована на сотрудниках организации, где было совершено преступление. В первую очередь отрабатываются связи сотрудника (вид служебной деятельности; близкие; знакомые, семья, хобби, увлечения, уровень доступа к компьютерной информации, а также уровень пользования и владения компьютерными программами).

В процессе раскрытия преступления тщательно проверяется вся информация, ставшая известной сотрудникам уголовного розыска от работников организации на месте. Устанавливаются прямые, промежуточные, случайные и закономерные связи и контакты между сотрудниками юридического лица.

Следует отметить, что залог успешной и эффективной оперативно-розыскной деятельности заключается в том, что стратегию и тактику раскрытия киберпреступлений необходимо строить на основе хороших знаний специфики составов преступлений, психологии, личности преступника, криминалистики и криминологии. Кроме того, соблюдение

[108] Харина, Э. Н. О возможностях использования сети Интернет при расследовании преступлений // Современное состояние и перспективы развития научной мысли : мат-лы междунар. науч.-практ. конф., г. Уфа, 25 мая 2015 года : в 2 ч. Ч. 2. Уфа, 2015. С. 132.

конспирации в оперативно-розыскной деятельности обеспечивает возможность установления и поимки преступников.

Конспиративность действий сотрудников уголовного розыска позволяет не допустить необоснованной или преждевременной компрометации объектов оперативной заинтересованности. Сохранение тайны в процессе оперативно-розыскной деятельности является обязательным условием конфиденциального содействия граждан оперативно-розыскным органам, обеспечивающим не только эффективность конфиденциального содействия, но и личную безопасность конфидентов, а также гарантией их специальных прав[109].

Организационные основы раскрытия преступлений, совершенных с помощью информационных технологий, представляют собой комплекс мер, методик и средств по созданию условий, необходимых для эффективного проведения оперативно-розыскных мероприятий.

В число этих мер входят обеспечение оперативно-тактической готовности органов внутренних дел к реагированию на сигналы о совершенных преступлениях; организация взаимодействия оперативных и следственных подразделений, участвующих в раскрытии преступлений; организация взаимодействия между смежными структурами, а также операторами, связи, интернет-провайдерами, кредитно-финансовыми организациями; осуществление постоянного оперативного контроля над лицами, состоящими на оперативных учетах.

Успешное раскрытие киберпреступлений возможно исключительно при осуществлении оперативно-розыскной деятельности и должной ее организации. К субъектам организации данной деятельности относятся руководители органов внутренних дел на региональном уровне, начальники оперативных подразделений и иные должностные лица. В процессе ее осуществления применяется целый комплекс специальных организационно-управленческих и организационно-тактических мер, который предметно регламентирован и направлен на решение задач по раскрытию преступлений.

Подводя итоги рассматриваемого вопроса, следует отметить, что пресечение и раскрытие цифровых преступлений носит многоплановый, комплексный характер. При этом важное значение имеют не только профессиональные знания и умения самого субъекта профилактики, но и уровень материальной оснащенности, организационно-управленческие и организационно-тактические возможности органов профилактики и предупреждения.

[109] Осипенко, А. Л. Указ. соч. С. 43.

§ 4. Виктимологическая профилактика преступлений, совершаемых с использованием информационных (цифровых) технологий

Как мы уже говорили, предупреждение цифровой преступности – это многоплановая задача, в решении которой принимают участие многие субъекты и заинтересованные лица. Одними из таких лиц выступают потенциальные жертвы киберпреступлений. Иными словами, виктимологическая профилактика цифровой преступности есть не что иное, как основа предупреждения преступлений, совершаемых в сфере информационных (цифровых) технологий.

Выступая на расширенном заседании коллегии МВД России 17 февраля 2022 года, Президент Российской Федерации В. В. Путин подчеркнул, что «в результате действий кибермошенников урон несут отечественные компании, что вызывает особую остроту общественной реакции. С потерями средств и накоплений, с невосполнимым моральным ущербом сталкиваются наши граждане. Жертвами преступников становятся пенсионеры, многодетные семьи, люди с ограниченными возможностями по здоровью». В целом глава государства указал на «необходимость совершенствования механизма взаимодействия МВД России с финансовыми организациями, операторами связи и другими структурами, работающими в сфере ИТТ»[110].

В свою очередь, министр внутренних дел Российской Федерации В. А. Колокольцев указал, что «на 70 % увеличилась штатная численность подразделений по противодействию преступлениям, совершенным с использованием ИТТ, однако успешная борьба с IT-преступностью возможна только при консолидации усилий правоохранительных органов, соответствующих регуляторов, а также с участием операторов связи и Интернет-провайдеров»[111].

XXI век назван веком информации, информационных технологий. Сегодня трудно представить работу государственных учреждений, банков и других социально значимых организаций без использования компьютерной информации. Однако эта информация подвержена большому риску. Существует большое количество злоумышленников, которые находятся в постоянном поиске уязвимых мест в компьютерных системах, пытаясь получить незаконный доступ к информации, составляющей большую ценность для учреждений, компаний и т. д. Данная деятельность преступников называется «киберпреступностью». Как мы уже подчеркивали, в российском законодательстве отсутствует понятие «киберпреступность». Интерпретируют ее только ученые,

---

[110] Расширенное заседание коллегии МВД России // Официальное интернет-представительство Президента России : сайт. URL: http://kremlin.ru/events/president/news/67795. Дата публикации: 17.02.2022.

[111] Там же.

занимающиеся данным направлением. Под «киберпреступностью» принято понимать «преступления в сфере компьютерной информации», «информационные преступления» и т. д.

В научной литературе отмечается, что под киберпреступлением можно понимать акт социальной девиации с целью нанесения экономического, политического, морального, идеологического, культурного и других видов ущерба индивиду, организации или государству посредством любого технического средства с доступом в Интернет[112].

Жертвами киберпреступлений могут стать различные категории граждан. Напомним, что Уголовный кодекс Российской Федерации к преступлениям в сфере компьютерной информации относит: неправомерный доступ к компьютерной информации; создание, использование и распространение вредоносных компьютерных программ; нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей; неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации.

Статистические показатели о числе лиц, официально признанных жертвами цифровых преступлений, заставляют снова и снова обращаться к вопросам необходимости повышения уровня защищенности граждан от киберпреступности.

Ущерб мировой экономики от киберпреступлений растет в геометрической прогрессии. На сегодняшний день оборот киберпреступности (388 миллиардов долларов) больше, чем оборот на глобальном черном рынке марихуаны, кокаина и героина вместе взятых (288 миллиардов долларов), и приближается к значению оборота глобального рынка наркотиков (411 миллиард долларов)[113].

Киберпреступления совершаются отдельными лицами или небольшими группами, а также преступными организациями, которые часто разбросаны по всему миру и совершают преступления в беспрецедентных масштабах.

Киберпреступность имеет необычную характеристику, жертва и преступник никогда не вступают в непосредственный контакт; во многих случаях преступников и жертв разделяют тысячи километров. В целях дальнейшего снижения вероятности обнаружения и преследования злоумышленники часто предпочитают работать в странах со слабым законодательством, где вопросы профилактики киберпреступности никак не регулируются.

---

[112] Швед, Н. А. Неправомерный доступ к компьютерной информации: уголовно-правовая защита в РФ и Республике Беларусь // Информационное право : науч. журн.. 2016. № 2. С. 30–34.

[113] Там же.

В основе борьбы с цифровой преступностью (как и с любым иным видом преступности) должна лежать деятельность, направленная на нейтрализацию негативного воздействия криминогенных факторов, способствующих развитию данного вида преступности. Кроме того, большим потенциалом обладает виктимологическая профилактика. Для того чтобы эффективно противодействовать цифровым преступлениям, необходимо пресекать негативное воздействие следующих факторов:

1. Несоразмерность роста цифровизации общества и цифровой грамотности населения Российской Федерации. Согласно статистическому сборнику «Информационное общество в Российской Федерации. 2019», в период с 2016 по 2018 годы включительно доступ к сети Интернет увеличился на 1,8 %: если в 2016 году доступ к сети Интернет имело 74,8 % населения, то в 2018 – уже 76,6 % соответственно[114]. Исследования показывают, что только 27 % россиян (каждый четвертый) обладают высоким уровнем цифровой грамотности. Из-за недостаточного уровня знаний и навыков в сфере цифровых технологий многие люди и организации оказались не готовы к работе в дистанционном формате в условиях самоизоляции. Аналитический центр НАФИ представляет результаты комплексной оценки текущего уровня сформированности компетенций цифровой экономики у населения России и их готовности к жизни в условиях цифровизации. Измерения уровня цифровой грамотности россиян проводились в 2018, 2019 годах, а также в начале 2020 года[115].

2. Увеличение аудитории социальных сетей и мессенджеров. На 1 января 2022 года население Российской Федерации составляет 145,6 миллионов человек[116]. В октябре 2022 года число активных авторов в социальных медиа в России составило 62,2 млн. Авторы написали более 1,5 млрд публичных сообщений – постов, репостов и комментариев (в октябре 2021 года – 1,1 млрд), в то время, как в 2019 году число активных авторов в социальных медиа в России составило 49 млн. Авторы написали 1,3 млрд публичных сообщений (постов, репостов и комментариев). Количество авторов и сообщений по каждой социальной сети позволяют оценить популярность площадок среди российских пользователей.

---

[114] Информационное общество в Российской Федераци. 2019 : стат. сборник / М. А. Сабельникова, Г. И. Абдрахманова, Л. М. Гохберг, О. Ю. Дудорова и др.; Федеральная служба государственной статистики; Нац. исслед. ун-т «Высшая школа экономики». Электрон. текст дан. (31,8 Мб). URL: https://rosstat.gov.ru/storage/mediabank/info-ob2019.pdf (дата обращения: 05.09.2023).

[115] Цифровая грамотность россиян: исследование 2020 // НАФИ. Аналитический центр : сайт. URL: https://nafi.ru/analytics/tsifrovaya-gramotnost-rossiyan-issledovanie-2020/ (дата обращения: 05.09.2023).

[116] Численность населения Российской Федерации по полу и возрасту на 1 января 2022 года : стат. бюллетень // Федеральная служба государственной статистики (Росстат) : сайт. URL: https://rosstat.gov.ru/storage/mediabank/Bul_chislen_nasel-pv_01-01-2022.pdf (дата обращения: 05.09.2023).

Очевиден прирост аудитории в социальном пространстве на 13,2 миллиона человек, что составляет 9,07 % от населения нашей страны[117].

3. Активный рост применения электронных средств платежей. Например, по сведениям Центрального банка России, количество распоряжений, которые составлены и переданы в электронном виде клиентам кредитных организаций и самой кредитной организации через сеть Интернет, за 2021 год составило 2 703,7 млн, а за аналогичный период 2020 года – 1 993,4 млн[118].

В данном случае можно заключить, что распространенность использования современных цифровых технологий не вызывает сомнений, и человек, использующий ИТТ, может с легкостью стать жертвой киберпреступления либо просто пострадать из-за отсутствия у него базовых правил цифровой безопасности, таких как:

1) Не переходить по ссылкам, отправленным ему через личные сообщения мессенджеров или социальных сетей, поскольку пользователь, отправивший их, может быть взломан, вследствие чего другому пришла ссылка на фишинговый сайт. В данном случае пользователь может получить материальный вред от кражи конфиденциальной информации или же искомых данных банковских карт.

2) При покупке на интернет-ресурсах, какой бы ни была привлекательной цена того или иного товара, не следует переводить предоплату, поскольку злоумышленники часто пользуются наивностью людей – это один из основных механизмов социальной инженерии.

3) Не стоит ставить один и тот же пароль на все свои интернет-ресурсы, будь то электронная почта или аккаунт от социальных сетей. Не следует также хранить пароли в любом электронном виде, так как телефон могут взломать дистанционно. Целесообразнее всего все свои пароли хранить на бумажных носителях или в голове.

4) В продолжение темы покупок в Интернете следует отметить, что необходимо завести отдельную банковскую карту, чтобы переводить на нее определенную сумму денежных средств, и в случае утечки банковских данных, то есть номера карты или трехзначного кода на обратной стороне, можно не волноваться, что абсолютно все денежные средства владельца будут похищены.

5) Не спешить заполнять анкеты, приходящие из неизвестных спам-рассылок. Вводить свои персональные данные следует только на проверенных сайтах, поскольку в противном случае данное заполнение может быть использовано не по назначению указанной анкеты.

---

[117] Социальные сети в России: цифры и тренды, осень 2022 // Brand Analytics : сайт. URL: https://br-analytics.ru/blog/social-media-russia-2022/ (дата обращения: 05.09.2023).

[118] Статистика национальной платежной системы // Банк России : сайт. URL: https://cbr.ru/statistics/nps/psrf/ (дата обращения: 05.09.2023).

6) Помнить о том, что киберзлоумышленники – хорошие манипуляторы, искусно пользующиеся приемами социальной инженерии. Они могут вызвать у потерпевшего чувство тревожности и стресса путем сообщения информации о чрезвычайном положении близких и родных или иных ситуациях, которые могут дестабилизировать жертву преступления.

7) Внимательно следить за теми файлами, которые скачиваются из неизвестных источников, при этом на том или ином устройстве обязательно должно быть установлено антивирусное программное обеспечение.

8) Проверять условия и права доступа при скачивании программ и файлов из неизвестных источников.

9) Своевременно обновлять антивирус, что предотвратит возможное установление вредоносного программного обеспечения.

Из этого следует, что всю входящую информацию следует пропускать через призму скептицизма. Не стоит доверять любой входящей информации, ведь впоследствии она может принести как материальный, так моральный вред.

ГЛАВА 7.
МЕЖДУНАРОДНЫЙ ОПЫТ СОТРУДНИЧЕСТВА ГОСУДАРСТВ ПО ПРЕДУПРЕЖДЕНИЮ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ (ЦИФРОВЫХ) ТЕХНОЛОГИЙ

§ 1. Основные направления международного сотрудничества государств в сфере предупреждения преступности в области информационных (цифровых) технологий

Преступность существовала со времен появления человеческого общества. К сожалению, никакие превентивные меры не помогли людям избавиться от преступности навсегда. При этом данная проблема характерна для всех стран мира, ни одно государство не избавило свое общество от преступности в полном объеме. Например, если обратиться к официальным статистическим данным Генеральной прокуратуры Российской Федерации, то можно заметить, что количественные и качественные показатели преступности в разных странах различны и обладают своими особенностями. Например, в Бразилии ежегодно совершается свыше 60 тысяч преднамеренных убийств; в США число нападений на граждан, в результате которых потерпевшим причиняется вред здоровью или смерть, составляет свыше 800 тысяч ежегодно; в Великобритании ежегодно совершается около полутора миллионов краж[119]. Поэтому можно сделать вывод, что ни одно государство мира не свободно от такого негативного явления, как преступность. В этой связи вопросы международного сотрудничества в борьбе с преступлениями являются актуальными для всего мирового сообщества.

Преступность порождает у населения паническое состояние, парализацию нормальной и социально полезной деятельности, препятствует функционированию органов власти и управления, а также способствует достижению антиобщественных целей. Именно поэтому очень важно развивать все возможные механизмы, которые могут помочь побороть преступность. В качестве одного из таких механизмов выступает институт взаимодействия различных субъектов и представителей различных государств.

Несомненно, главная роль в вопросах противодействия преступности отводится органам полиции. При этом полицейские большинства стран мира давно научились эффективно взаимодействовать между собой, имея цель ликвидировать преступность. Однако становление и развитие

[119] Количество осужденных лиц // Генеральная прокуратура Российской Федерации. Портал правовой статистики : сайт. URL: http://crimestat.ru/world_ranking_convicted (дата обращения: 13.02.2023).

института международного сотрудничества подразделений ОВД в борьбе с преступностью, в том числе цифровой, имеет длительную историю, в том числе в рамках истории формирования взаимодействия различных субъектов, поскольку такое взаимодействие всегда широко и обширно, и в нем нередко участвуют различные органы разных государств.

С появлением новых видов преступлений, наносящих ущерб как отдельным государствам, так и международному сообществу в целом, государства незамедлительно принимают меры по борьбе с такими угрозами. В частности, новыми вызовами XXI века являются киберпреступления, поэтому в настоящее время усилия государств направлены на противодействие преступным деяниям в сфере высоких технологий. Как верно отмечают специалисты, современные цифровые технологии предопределили возникновение новых подходов к организации оперативно-розыскной деятельности, в том числе на международном уровне[120].

Иными словами, следует констатировать, что историческое развитие различных аспектов международного сотрудничества в вопросах борьбы с преступностью всегда обуславливается современными жизненными реалиями. Международное сотрудничество развивается тогда, когда это становится необходимо для различных представителей зарубежных государств. И в этом процессе, несомненно, задействуются представители органов внутренних дел.

Поскольку цифровые преступные деяния могут быть совершены вне пределов нашей страны, то есть из других государств путем тех или иных кибермошеннических атак, был принят ряд международных соглашений и договоров по борьбе с преступлениями в цифровой сфере.

Для того чтобы данные международные документы эффективно применялись различными государствами, требуется унификация международного законодательства в сфере киберпреступлений, которая не только даст возможность предотвратить создание безопасных убежищ для киберпреступников, но и исключит возможность избежать серьезного наказания за совершение киберпреступлений. Как заявляют представители Организации Объединенных Наций (далее – ООН), подобные безопасные убежища создаются потому, что лишь те действия, которые превышают порог тяжких преступлений, – который, как правило, выражается в форме возможного наказания, которое может повлечь за собой соответствующее деяние, – оправдывают вложения, необходимые для осуществления

[120] Тимофеев, С. В., Лузько, Д. Н. Особенности сбора оперативно-розыскной информации: международная и отечественная практика // Криминалистика: вчера, сегодня, завтра : сб. науч. тр. 2022. № 3 (23). С. 132.

международного сотрудничества[121]. Таким образом, развитию международного сотрудничества будет способствовать унификация основных положений законов о киберпреступности.

Международное сотрудничество – это взаимодействие между государствами, на основании и в рамках принятых ими международных соглашений, конвенций и иных нормативных правовых актов, которые регулируют те или иные вопросы деятельности субъектов данных нормативных правовых актов[122].

Так, по поводу международного сотрудничества государств в рамках предупреждения преступлений в цифровом пространстве необходимо выделить цели данного взаимодействия:

1. Разработка и принятие унифицированной нормативно-правовой базы документов, регулирующих правоотношения, возникающие в связи с совершением преступления, которое сопряжено с применением компьютеров и компьютерных систем.

2. Создание ряда положений и инструкций по противодействию кибератакам на персональные данные.

3. Разработка специальных программ для компьютерных систем, необходимых для защиты персональных данных.

4. Создание международной системы безопасности, подразумевающей интеграцию всех мер предосторожности по обращению с компьютерными сетями, а также включающей в себя стандарты, необходимые для обеспечения информационной безопасности пользователя.

В соответствии с Конвенцией о преступности в сфере компьютерной информации[123], принятой Советом Европы, под киберпреступлениями следует понимать противоправные посягательства, направленные на нарушение конфиденциальности, целостности и допустимости компьютерных сведений и систем. К таким преступным деяниям специалисты относят следующие:

1) незаконный доступ (ст. 2);

2) незаконный перехват (ст. 3);

3) вмешательство в данные (ст. 4);

4) вмешательство в систему (ст. 5).

---

[121] Киберпреступность. Правовая база и права человека. Управление Организации Объединенных Наций по наркотикам и преступности. Вена, 2019. Электр. версия. URL: https://www.unodc.org/documents/e4j/Cybercrime/Cybercrime_Module_3_Legal_Frameworks_and_Human_Rights_RU.pdf (дата обращения: 18.01.2023).

[122] Жужгина, А. А. Международное сотрудничество в сфере уголовного процесса: проблемы экстрадиции киберпреступников // Молодой ученый : науч. журн. 2020. № 21 (311). С. 305.

[123] Конвенция о преступности в сфере компьютерной информации ETS № 185 : заключена в г. Будапеште 23 ноября 2001 года // Гарант : сайт. URL: https://base.garant.ru/4089723/?ysclid=lmdbuavnd1100821049 (дата обращения: 18.01.2023). Российская Федерация в настоящей Конвенции не участвует.

Примечательны мнения и отечественных правоведов. Например, М. Е. Бегларян отождествляет термины «интернет-преступление» и «киберпреступление», понимая под ними «полный перечень общественно опасных действий в области информационных технологий»[124].

М. Е. Батухтин утверждает следующее: «киберпреступление – это любое уголовно наказуемое деяние, выраженное в электронной форме, совершенное с использованием компьютерных устройств или виртуальной сети, а также против них»[125].

Проанализировав вышеперечисленные определения киберпреступлений, закрепленные в международных нормативных правовых актах и отраженные в научно-исследовательских трудах отечественных ученных, можно прийти к выводу, что рассматриваемая разновидность преступности делится на две категории:

1) компьютерные преступления;

2) преступные посягательства, совершаемые в киберпространстве.

Подчеркнем, что в первую очередь международное сотрудничество России с иными странами осуществляется посредством деятельности ООН. Российская Федерация как член ООН является участницей практически всех международных конвенций и соглашений по борьбе с преступностью.

Например, Конвенция ООН против транснациональной организованной преступности, принятая резолюцией 55/25 Генеральной Ассамблеи от 15 ноября 2000 года[126], была ратифицирована Российской Федерацией и имплементирована в российское правовое поле[127]. Данный документ также затрагивает вопросы по международному

---

[124] Бегларян, М. Е., Войтова-Долгих, Я. Н., Одинцов, С. А. Исторические аспекты понятий «киберпреступление» и «кибертерроризм» в законодательстве: проблемы трактования // Научный вестник : науч. журн. 2020. № 4 (50). С. 15.

[125] Батухтин, М. Е. Киберпреступления: причины, виды, формы, последствия, направления противодействия // Проблемы и перспективы развития уголовно-исполнительной системы России на современном этапе : мат-лы междунар. науч. конф. адъюнктов, аспирантов, курсантов и студентов, г. Самара, 27 апреля 2018 года : в 3 ч. 2018. Ч. 3. С. 5.

[126] Конвенция Организации Объединенных Наций против транснациональной организованной преступности : принята резолюцией 55/25 Генеральной Ассамблеи от 15 ноября 2000 года // Организация Объединенных Наций : сайт. URL: https://www.un.org/ru/documents/decl_conv/conventions/orgcrime.shtml (дата обращения: 21.06.2023).

[127] О ратификации Конвенции Организации Объединенных Наций против транснациональной организованной преступности и дополняющих ее протокола против незаконного ввоза мигрантов по суше, морю и воздуху и протокола о предупреждении и пресечении торговли людьми, особенно женщинами и детьми, и наказании за нее : Федер. закон № 26-ФЗ : принят Гос. Думой 24 марта 2004 года : одобрен Советом Федерации 14 апреля 2004 года // Официальный интернет-портал правовой информации : сайт. URL: http://pravo.gov.ru/proxy/ips/?docbody=&firstDoc=1&lastDoc=1&nd=102086543 (дата обращения: 21.06.2023).

сотрудничеству в борьбе с межнациональными преступлениями, к которым следует относить и цифровые преступления.

Генеральной Ассамблеей и Советом Безопасности ООН были приняты десятки резолюций по таким вопросам, как пресечение финансирования терроризма, борьба с ОМУ (оружие массового уничтожения), терроризмом, бомбовым терроризмом, подстрекательством к совершению террористических актов, захватом заложников и т. д.

В настоящем пособии мы неоднократно обращали внимание на то, что одним из актуальных цифровых преступлений является финансирование террористической деятельности посредством использования цифровых технологий. На международном уровне представители различных государств неоднократно обращали внимание на необходимость совместной борьбы с терроризмом. К сожалению, терроризм стал обычной характерной чертой новейшей истории многих зарубежных государств, и его отрицательные последствия вызывают существенный социальный резонанс. Терроризм считается негативным общественным явлением, которое требует прежде всего осмысления ключевых аспектов имеющейся проблемы. Начиная с 70-х годов XX века, практически ежегодно проблема борьбы с терроризмом входила в повестку дня Генеральной Ассамблеи и Совета Безопасности ООН. Примечательно, что в текстах их резолюций в качестве субъекта преступления терроризма были указаны как физические лица, так и государства[128]. Особое внимание в таких документах уделяется безопасности гражданской авиации, морского судоходства и ряду других вопросов[129].

Если говорить о международном терроризме, то он посягает не просто на интересы двух и более государств, а на весь мир и международную безопасность. Вместе с тем в настоящее время международный терроризм квалифицируется как преступление международного характера. Россия, вступив на путь рыночных отношений, открыла огромные возможности для развития преступности, в том числе международного терроризма. Это особо опасное социально-политическое явление, которое способствует подрыву национальной безопасности разных стран. В настоящее время основная проблема преступлений террористической направленности состоит в увеличении числа форм их проявления, что, безусловно, представляет серьезную угрозу как для России, так и для мирового сообщества в целом, для жизнедеятельности мирового сообщества и национальной безопасности разных стран.

[128] Абрамова, А. А. Взаимодействие органов предварительного расследования Российской Федерации с международными органами и организациями при расследовании преступлений о финансировании терроризма // Общество: политика, экономика, право : науч. журн. 2021. № 11 (100). С. 60.

[129] Нэх, В. Ф. Особенности борьбы советских органов безопасности с политическим терроризмом в советской России и СССР (1917-1991 гг.) // Военный академический журнал : науч. журн. 2020. № 2 (26). С. 41.

Терроризм выступает одним из главных факторов, дестабилизирующих ситуацию не только в нашей стране, но и во всем мире. Террористические преступления преимущественно совершаются наиболее опасным способом, который приводит к тяжким последствиям. Использование террористами устройств с большим количеством взрывчатых веществ, совершение преступлений террористической направленности в местах массового скопления людей влечет существенные потери.

В этой связи о необходимости совершенствования правового регулирования предупреждения терроризма говорится во многих международных актах, в том числе принятых в рамках работы ООН. При Совете Безопасности ООН работает несколько целевых комитетов, например Комитет 1267. Государства-члены принимают меры по предотвращению террористической деятельности, объявлению различных форм террористической деятельности противозаконными, а также меры для установления двустороннего и многостороннего сотрудничества в целях предотвращения и пресечения террористических нападений[130].

При международном взаимодействии тех или иных субъектов, в том числе представителей оперативных подразделений полиции разных стран, ведущая роль принадлежит ООН. Так, например, в 2013 г. XXII сессия Комиссии касалась проблем, связанных с новыми видами преступлений, оказывающих существенное отрицательное воздействие на окружающую среду, и способов борьбы с такими преступлениями. В 2014 г. тематика XXIII сессии Комиссии – международное сотрудничество по вопросам уголовного правосудия, в рамках которого происходит обсуждение актуальных проблем, связанных с преступностью, выработка согласованных планов, программ действий, нацеленных на борьбу с преступностью, разработка соответствующих международных правовых документов. Подобные межправительственные форумы оказывают влияние на национальную политику разных стран. Более того, наряду со структурными звеньями ООН, занимающимися непосредственно вопросами международного взаимодействия в борьбе с преступностью, в рамках своей компетенции таким вопросам уделяется внимание и со стороны некоторых специализированных учреждений системы ООН: Международной организации гражданской авиации – ИКАО, Всемирной организации здравоохранения – ВОЗ и других.

[130] Горюнкова, Н. А. Специфика осуществления взаимодействия подразделений по противодействию экстремизму МВД России с правоохранительными органами зарубежных стран в сфере противодействия террористическим проявлениям // Вестник Всероссийского института повышения квалификации сотрудников МВД России : науч.-практ. журн. 2019. № 4 (52). С. 89.

Как мы уже подчеркивали, в масштабах мирового сообщества международное сотрудничество осуществляется под эгидой ООН. Например, можно обратить внимание на международный уровень борьбы с рабством. Следует отметить, что реалии современного мира обусловили новый подход к такому явлению, как рабство и работорговля, придав ему расширительное толкование. Проблема торговли людьми в российском законодательстве была обозначена еще в XIX веке. Уголовное уложение Российской империи 1903 года признавало ответственность за продажу людей в рабство другим иноплеменникам. Среди преступлений с тяжкими последствиями наиболее распространенными оставались похищение женщин с целью изнасилования, а также насильного вступления в брак.

Долгое время уголовное законодательство новой России не сталкивалось с понятием торговли людьми, однако в действующем уголовном законодательстве содержатся нормы о торговле людьми. На международном съезде Государственной Думы 1997 года, исследователями-правоведами был представлен доклад о проблеме, приобретшей глобальные масштабы, в которым был сформулирован запрет вывоза людей, а в особенности лиц женского пола, с целью сексуальной эксплуатации. На протяжении шести лет представители организаций международного характера, российских неправительственных организаций, сообществ и объединений, ученые и диссиденты убеждали в необходимости введения уголовно-правового запрета торговли людьми и использования рабского труда.

Подчеркнем, что на современном этапе развития общества преступная деятельность, связанная с работорговлей, обязательно сопряжена с цифровыми технологиями. И в этой связи в целом борьба с киберпреступностью, реализация эффективных мер защиты от информационных угроз будет способствовать снижению количества преступлений, посягающих на различные блага и ценности человека, в том числе на его свободу.

Каждый международный договор в сфере борьбы с рабством и работорговлей, начиная от Конвенции относительно рабства 1926 г.[131], заканчивая Протоколом о предупреждении и пресечении торговли людьми, особенно женщинами и детьми, и наказании за нее, дополняющим Конвенцию ООН против транснациональной организованной преступности 2000 г., содержит ряд обязательств для государств, призванных предотвращать, раскрывать, расследовать данные преступные деяния и бороться с ними.

---

[131] Конвенция относительно рабства : подписана в Женеве 25 сентября 1926 года : с изменениями, внесенными Протоколом от 7 декабря 1953 года // Кодекс: Электронный фонд правовых и нормативно-технических документов : сайт. URL: https://docs.cntd.ru/document/1901044?ysclid=lmdbpbzxi8910366579 (дата обращения: 21.03.2023).

Последним документом по времени принятия и своей универсальной масштабности является разработанный ООН Глобальный план действий по борьбе с торговлей людьми[132]. Документ отражает несколько направлений сотрудничества государств:

– разработка широких программ и стратегий в рамках ООН в области развития прав человека и их претворение в жизнь на национальном уровне;

– исследование, сбор информации и ее последующий анализ по вопросам масштаба и характера проблемы;

– информационно-разъяснительные кампании, ориентированные на лиц, могущих стать жертвами преступления;

– информирование населения о правах человека в качестве предупреждения торговли людьми;

– защита жертв преступления;

– установление на национальном уровне уголовно-правовой ответственности за рассматриваемые преступления.

Торговля людьми представляет собой крайне опасное преступление против прав человека наряду с другими противоправными действиями, связанными с продажей оружия и наркотиков, привлекает к себе гораздо больше внимания, ведь объектом в таких преступных деяниях выступает сам человек.

Именно поэтому борьба с торговлей осуществляется двумя путями: предупреждение преступлений и пресечение попыток совершения преступлений со стороны уголовного правосудия, а также приложение немалых усилий в области прав человека и гражданина с целью защиты прав граждан, ставших объектами торговли. Вопросы международного полицейского сотрудничества в данном вопросе приобретают большое практическое значение, поскольку от оперативных профессиональных действий правоохранительных органов будут зависеть жизни конкретных людей, ставших жертвами торговли людьми.

Помимо названных существуют так называемые региональные формы международного сотрудничества в сфере предупреждения цифровой преступности. Подчеркнем, что за последние годы региональное сотрудничество в области противодействия цифровой преступности стало более продуктивным.

Так, Советом Европы были приняты Конвенция о преступности в сфере компьютерной информации (которую мы упоминали ранее),

---

[132] Глобальный план действий Организации Объединенных Наций по борьбе с торговлей людьми : принят резолюцией 64/293 Генеральной Ассамблеи ООН от 30 июля 2010 года // Организация Объединенных Наций : сайт. URL: https://www.un.org/ru/documents/decl_conv/conventions/gp_trafficking.shtml (дата обращения: 21.06.2023).

соответствующая Резолюция[133] и Декларация[134], направленные на построение безопасного информационного общества. Они сегодня определяют уголовно-правовую политику мирового сообщества, нацеленную на защиту общества от преступлений, совершаемых в сфере цифровых технологий, путем подготовки нормативных правовых актов и укрепления сотрудничества международного сообщества в указанной сфере.

Иными словами, речь идет об отдельных видах межгосударственного взаимодействия. Стоит отметить, что Российская Федерация активно принимает участие в региональном международном сотрудничестве. Например, 1 июля 2021 года был принят Федеральный закон № 237-ФЗ «О ратификации Соглашения о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий»[135].

Еще один немаловажный международный инструмент в борьбе с цифровой преступностью – это деятельность межправительственной организации, которая занимается выработкой мировых стандартов в сфере противодействия отмыванию преступных доходов и финансированию терроризма, а также осуществляет оценки соответствия национальных систем этим стандартам. Речь идет о группе разработок финансовых мер борьбы с отмыванием денег (ФАТФ – от англ. «Financial Action Task Force on Money Laundering (FATF)»). За последние годы ФАТФ неоднократно обращала внимание на проблемы идентификации личности. Так, ею подготовлено Руководство о цифровой идентификации личности, которое в марте 2020 г. было направлено во все страны-участницы[136].

---

[133] Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности : резолюция A/RES/53/70 от 4 января 1999 года // Организация Объединенных Наций : сайт. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N99/760/05/PDF/N9976005.pdf?OpenElement (дата обращения: 21.06.2023).

[134] Декларация принципов «Построение информационного общества – глобальная задача в новом тысячелетии» : принята в Женеве 12 декабря 2003 года // Организация Объединенных Наций : сайт. URL: https://www.un.org/ru/events/pastevents/pdf/dec_wsis.pdf (дата обращения: 18.01.2023).

[135] О ратификации Соглашения о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий : Федер. закон № 237-ФЗ : принят Гос. Думой 15 июня 2021 года : одобрен Советом Федерации 23 июня 2021 года // Официальный интернет-портал правовой информации : сайт. URL: http://www.pravo.gov.ru/proxy/ips/?docbody=&prevDoc=603211409&backlink=1&nd=602263581&rdk= (дата обращения: 21.06.2023).

[136] Руководство ФАТФ. Цифровая идентификация. Март 2020 // Международный учебно-методический центр финансового мониторинга : сайт. URL: https://mumcfm.ru/mediateka/86?format=document (дата обращения: 02.06.2023).

Исходя из содержания указанных международных нормативных правовых актов, можно выделить следующие направления международного сотрудничества в сфере предупреждения цифровой преступности, которые соответствуют целям, указанным выше:

1. Установление, разработка, согласование между государствами-участниками и принятие необходимых мер по предупреждению цифровых преступлений, независимо от их территориальности.

2. Отслеживание и выискивание возможных и готовящихся угроз для цифровой безопасности всего мирового сообщества.

3. Разработка унифицированного законодательства, регулирующего область кибербезопасности, что в сфере материального права выражается в виде мер наказания (их видов и размеров), а в сфере процессуального права подразумевает, например, меры о соответствующей подсудности и подведомственности уголовных дел.

4. Создание, согласование и утверждение курса по предостережению совершения преступлений, связанных с применением цифровых технологий.

5. Разработка и налаживание постоянного обмена информацией по готовящимся, совершающимся или совершенным киберпреступлениям с целью их будущего пресечения.

6. Обмен опытом между уполномоченными компетентными сотрудниками, трудящимися в сфере борьбы с преступлениями, связанными с компьютерными сетями и вредоносным программным обеспечением.

7. Обмен знаниями и опытом между студентами разных стран, учащимися в научно-исследовательских институтах, имеющих узкую направленность в сфере обеспечения кибербезопасности государства.

8. Создание иных условий для международного сотрудничества правоохранительных органов государств-участников.

Для реализации обозначенных направлений и эффективного межгосударственного сотрудничества необходимо в первую очередь постараться решить внутригосударственные проблемы, связанные с раскрытием преступлений цифрового характера. К таким проблемам можно отнести:

1) Высокий уровень латентности цифровых преступлений, который связан с тем, что потерпевшие граждане не обращаются в правоохранительные органы из-за несовершения преступления до конца, или же малозначительности ущерба, причиненного владельцу тех или иных данных или электронных денежных средств. Для того чтобы преодолеть подобное субъективное отношение потерпевшего к противоправному деянию, необходимо формировать в обществе нетерпимость к проявлению противозаконного поведения, даже если речь идет о незначительной сумме денежных средств. Это необходимо для того,

чтобы лица, ставшие жертвами того или иного цифрового преступления, обращались в правоохранительные органы для уменьшения процента латентности данных составов преступлений.

2) Отток кадров современной правоохранительной системы. Нередко можно услышать, что, например, в системе МВД происходит кадровый голод, нет достаточного количества сотрудников, которые обладают специальными познаниями в цифровой сфере, кибербезопасности. Кроме того, данная проблема усугубляется еще одной – недостаточной подготовкой сотрудников, которая неразрывно связана с отсутствием необходимого технического обеспечения. Если проводить сравнение с материальной обеспеченностью преступников, то можно заметить, что в преступной цифровой среде регулярно происходит цифровой прирост технических средств, которые позволяют совершать все более изощренные преступления в сфере информационного поля.

3) Разрозненность действий правоохранительных органов, иных государственных органов, учреждений и представителей общества. Данную разрозненность можно устранить путем принятия межведомственных инструкций, которые должны будут упрощать взаимодействие между указанными субъектами. Например, если правоохранительные органы запрашивают тот или иной документ у неподведомственного органа или организации, то такое предоставление документов, как правило, занимает большой промежуток времени, поскольку зачастую связано с длительным этапом согласования для выдачи данного документа, имеющего значение для решения неотложных уголовно-процессуальных задач.

4) Несовершенство законодательства. К сожалению, законодательство в сфере противодействия киберпреступлениям на сегодняшний день несовершенно. Например, не установлена уголовная ответственность за фишинг, под которым понимаются действия, ориентированные на неправомерное получение доступа к конфиденциальным данным пользователей, прежде всего к логинам и паролям. Также не закреплена уголовная ответственность за рассылку вредоносного спама.

5) Низкий уровень цифровой грамотности населения, о чем говорилось ранее. Чтобы решить данный вопрос, необходимо, чтобы правоохранительные органы эффективно сотрудничали со средствами массовой информации. СМИ обладают большим потенциалом в вопросе информационной грамотности, что, несомненно, окажет положительный эффект на цифровую просвещенность нашего населения.

Таким образом, для решения вышеперечисленных проблем необходимы:

– разработка, согласование и принятие актуальных правовых предписаний, регулирующих вопросы борьбы с цифровыми преступными посягательствами, в том числе на международном уровне;

– международный обмен кадрами для передачи наработанного положительного опыта между ведущими специалистами, дальнейшей разработки методических материалов по урегулированию вопросов уголовно-правового характера на международном уровне.

«С 2018 года ежегодно в Москве в Центре международной торговли проводится International Cybersecurity Congress (ICC), участие в котором принимают спикеры более чем из 50 стран, включая представителей государственных структур, международных организаций, ведущих специалистов и экспертов в области обеспечения информационной безопасности экономического цифрового пространства. В 2019 году на международном конгрессе по кибербезопасности в своем обращении премьер-министр Д. А. Медведев сформулировал основные задачи по противодействию киберпреступности:

– укрепление законодательной базы и разработка мер по борьбе с кибератаками;

– установление стандартов защиты цифровых отраслей;

– стимулирование создания отечественного программного обеспечения;

– выработка общих мировых стандартов обеспечения безопасности, так как киберпреступность не имеет границ.

Участие в конгрессе представителей Интерпола, Европола, участников Всемирного экономического форума говорит о рассмотрении данного вопроса на международном уровне»[137].

Исходя из всего вышесказанного, можно заключить, что борьба с цифровыми преступлениями, в том числе на международном уровне, – это сложная организационно-правовая система, которая требует долгого создания, согласования и утверждения соответствующих мер реагирования. Актуальным остается вопрос международного сотрудничества в борьбе с цифровой преступностью. При этом данное сотрудничество зависит не только от внешней политики государства, но и от готовности самого государства к созданию благоприятных условий для сотрудничества в сфере предупреждения цифровых преступлений.

[137] Маслиенко, М. А. Киберпреступность на современном этапе // Проблемы правоохранительной деятельности : науч. журн. 2021. № 2. С. 30.

§ 2. Роль органов внутренних дел в международном сотрудничестве по вопросам борьбы с преступлениями, совершаемыми с использованием информационных (цифровых) технологий

Статья 2 Конституции Российской Федерации обязывает государство признавать, уважать и защищать права и свободы человека и гражданина. Это полностью соответствует верховенству права, провозглашенному в статье 1 Конституции. Из вышеприведенных положений следует, что государство должно привлекаться к деятельности, направленной на борьбу с преступностью. Такое привлечение реализуется в первую очередь в форме работы соответствующих субъектов, к числу которых относятся подразделения ОВД.

Как свидетельствуют современные реалии, правоохранительные органы все чаще вынуждены реагировать на криминальные вызовы и угрозы. Одной из таких угроз выступает цифровая преступность, борясь с которой, подразделения ОВД используют в своей деятельности различные инструменты, в том числе механизм международного сотрудничества. Подчеркнем, что международное сотрудничество имеет длительную историю своего развития.

Исследование вопроса об истории становления и развития международного сотрудничества подразделений ОВД в борьбе с преступностью, в том числе цифровой, показывает, что данный институт (институт сотрудничества представителей различных государств в борьбе с преступлениями) строится на взаимодействии не только работников оперативных подразделений, но и представителей иных государственных и негосударственных организаций. Объясняется это тем, что международная, межгосударственная преступность очень обширна и может затрагивать интересы различных субъектов. В этой связи и борьба с преступностью должна осуществляться с привлечением как можно большего количества субъектов. Иными словами, в такой криминальной борьбе требуется взаимодействие как оперативных подразделений разных стран, так и иных представителей иностранных государств.

Вопрос взаимодействия представителей ОВД различных стран при осуществлении противодействия цифровым преступлениям является актуальным потому, что сама суть цифровых преступлений нередко кроется в международном, трансграничном характере. Цифровое преступление – это действие, совершенное хорошо осведомленным пользователем компьютера, иногда называемым хакером, который незаконно просматривает или крадет личную информацию компании или отдельного лица. В некоторых случаях это лицо или группа лиц могут быть злонамеренными и уничтожить или иным образом повредить компьютер или файлы данных. В качестве альтернативы их называют

киберпреступностью, электронной преступностью, компьютерной преступностью, высокотехнологичной преступностью, цифровой преступностью.

Киберпреступность, реализуемая посредством сети Интернет, приобретает массовый характер по мере того, как компьютер занимает ведущее место в торговле, развлечениях и управлении государством. При киберпреступности, также называемой цифровой преступностью, компьютер (гаджет) является ключевым инструментом для достижения незаконных целей, таких как мошенничество, торговля детской порнографией и интеллектуальной собственностью, кража личных данных или нарушение конфиденциальности.

Учитывая распространенность киберпреступлений и масштабность проникновения цифровых технологий в современную жизнь практически каждого человека в современном обществе, следует выстраивать соответствующую превентивную деятельность, исходя именно из этого. Превентивные меры, реализуемые сотрудниками органов внутренних дел, в том числе при осуществлении международного сотрудничества по вопросам борьбы с цифровыми преступлениями, должны быть направлены не только на выявление уже совершенных киберпреступлений, но и на раннюю профилактику, а для этого необходимо эффективно воздействовать на те факторы, которые способствуют совершению преступлений в сфере ИТТ.

Во-первых, одним из ключевых факторов совершения данной категории преступлений выступает глобальная (повсеместная) цифровизация общества, т. е. тотальное внедрение цифровых технологий в различные сферы жизни общества и его хозяйственной деятельности, и это необходимо учитывать в работе по предупреждению подобных преступлений. Целесообразным является использование данных технологий «в плюс», в частности, в сети Интернет можно распространять информацию, направленную на виктимологическую профилактику цифровой преступности, и в таких случаях цифровые технологии уже будут помогать, а не мешать сотрудникам правоохранительных органов в борьбе с киберпреступлениями.

Во-вторых, в настоящее время присутствует всеобщая доступность компьютерных технологий как для физических, так и для юридических лиц (организаций), как правило, хранящих и аккумулирующих личную, коммерческую и иную информацию на различных цифровых носителях. По сути, многие сферы общественной жизни ушли в киберпространство, что, с одной стороны, послужило драйвером развития цифровых услуг, а с другой стороны, расширило возможности для преступной деятельности.

В-третьих, самым важным фактором, создающим условия и возможности для деятельности киберпреступников, по-прежнему остается низкая цифровая грамотность и низкий уровень кибербезопасности как граждан, так и организаций. Указанные факторы обусловили в последние годы всплеск преступлений в сфере цифрового пространства.

Подчеркнем, что лица, совершающие противоправные деяния в сфере цифрового пространства, используют различные инструменты и способы противодействия пресечению и раскрытию уголовно наказуемых посягательств в данной области. И представители правоохранительных органов должны работать «на опережение», в том числе используя механизмы международного сотрудничества.

Международное сотрудничество по вопросам борьбы с преступностью, как мы уже говорили, строится на взаимодействии различных субъектов профилактики.

Вместе с тем, если мы хотим подчеркнуть такой аспект международного взаимодействия, как сотрудничество подразделений органов внутренних дел различных государств, можно использовать устоявшиеся в научной литературе термины «международное полицейское сотрудничество» и «международное сотрудничество оперативных аппаратов».

Важно обратить внимание на значимость именно полицейского сотрудничества, т. е. сотрудничества между представителями правоохранительных полицейских органов разных стран. Из всех существующих правоохранительных и других государственных органов именно органам внутренних дел необходимо приводить в действие существующие предупредительные меры. Данный факт объясняется тем, что именно в полицию поступают первоначальные сведения о совершенных преступлениях, и потом уже полиция выполняет определенную работу по предупреждению преступности в отношении определенных лиц.

Министерство внутренних дел Российской Федерации, по нашему мнению, занимает очень важное место в системе предупреждения цифровых преступлений. Это связанно с тем, что представители органов внутренних дел часто занимаются профилактическими и иными беседами с гражданами, криминологическим предупреждением, общаясь непосредственно с участниками преступного мира, а также показывают людям яркие примеры осуществления преступной деятельности.

Основная задача органов внутренних дел – предупреждать преступность. При этом ОВД, осуществляя свою деятельность по раскрытию и расследованию преступлений, опираются на помощь иных служб, деятельность которых связана с преступлениями, а также на помощь общественных объединений и, конечно же, граждан. Впервые идея создания единой полицейской службы на территории Европейского Союза была закреплена в 1992 г. в Маастрихтском договоре, положившем начало существованию самого Евросоюза.

Важно отметить, что в настоящее время растет роль подразделений органов внутренних дел в борьбе с цифровой преступностью. Особенно ярко это проявляется в момент, когда в той или иной стране начинаются

какие-либо беспорядки, наблюдаются проявления терроризма, экстремизма. В этих и похожих напряженных условиях именно полиция принимает на себя сильный удар и осуществляет немедленные действия для того, чтобы страна жила в покое и гармонии, чтобы преступная деятельность практически не касалась граждан. И в такой предупредительной деятельности значительная роль принадлежит международному сотрудничеству по вопросам борьбы с преступностью.

Очень важное значение в предупреждении преступлений правоохранительными органами имеет поддержание связи с международными общественными и иными объединениями, которые готовы помогать органам внутренних дел. Именно этот момент имеет главное значение в предупреждении преступной деятельности.

Международное полицейское сотрудничество – это объединение усилий органов полиции различных государств в интересах повышения эффективности стратегии и тактики ее действий по предупреждению, пресечению и расследованию правонарушений, а также принятию мер по совершенствованию управления полицейскими силами, кадрового, научно-методического и технического обеспечения их работы.

Сейчас существуют следующие основные формы полицейского сотрудничества на международном уровне:

– обмен оперативной информацией об организованной преступности;

– сотрудничество в специальных оперативных вопросах;

– проведение оперативно-розыскных мероприятий и следственных действий;

– перемещение свидетелей из одной страны в другую;

– взаимная правовая помощь в конспирации прибылей от противозаконной деятельности;

– проведение совместных оперативно-профилактических мероприятий;

– привлечение зарубежных специалистов для проведения экспертиз и различного рода консультаций;

– общение, стажировка и переподготовка иностранных коллег;

– предоставление средств техники, связи, вооружения.

В настоящее время отмечается рост именно киберпреступлений, в том числе международного характера (транснациональных преступлений), посягающих на сферу экономики, а также преступлений, посягающих на права и свободы человека, о чем свидетельствуют актуальные межгосударственные соглашения о борьбе с транснациональной преступностью, рабством и работорговлей и т. д.

Изучение универсальных механизмов противодействия преступности и определение самых актуальных направлений взаимодействия государств в данной сфере под эгидой ООН позволяет

сформулировать следующий вывод: ООН разработана мощная правовая база универсального характера, включающая в себя правовые акты как обязательного, так и рекомендательного характера. При этом помимо правовых механизмов противодействия преступности при ООН созданы специальные структуры и структурные подразделения по противодействию тем или иным преступным проявлениям.

Немаловажная роль в таком сотрудничестве отводится именно подразделениям полиции различных государств. При этом в основе полицейского сотрудничества лежат те или иные правовые акты, на основании которых происходит оказание государствами, в том числе подразделениями ОВД, правовой помощи друг другу.

В вопросах полицейского международного сотрудничества большое внимание уделяется борьбе именно с организованной преступностью, в том числе носящей характер киберпреступлений. В условиях глобализации организованная преступность приобрела ряд абсолютно новых параметров, что привело к изменению подходов к ее теоретическому осмыслению. Теперь организованную преступность следует понимать и рассматривать как явление многомерное и многообразное, оценка которого с криминологической точки зрения предполагает обновление методологического инструментария его изучения. Рассматривая организованную преступность, нельзя не отметить, что она представляет собой очень опасное социальное явление. Кроме исключительной степени общественной опасности организованная преступность отличается наличием структурной организации и целей, для достижения которых она возникает. Предупреждение как групповой, так и организованной преступности осуществляется в процессе сотрудничества России со спецслужбами других стран, которое включает взаимную правовую помощь, планирование, организацию совместной деятельности и т. д.

Продолжая исследование вопроса о полицейском международном сотрудничестве в вопросах борьбы с цифровыми преступлениями, отметим, что в мире широко известна Международная организация уголовной полиции – Интерпол, которая объединяет криминальную полицию 192 государств.

Представительство Интерпола есть во многих странах мира, например, существует Американское полицейское сообщество (Америпол). Данное сообщество является одной из региональных международных полицейских организаций. Руководителем Америпола является Генеральный Секретарь, основная функция которого заключается в представительстве этой организации на международной арене. В его полномочия также входят координация и контроль успешного развития сотрудничества в области борьбы с международной преступностью среди государств-участников на уровне полицейских и межправительственных подразделений Организации. Несмотря на значимую роль Генерального

Секретаря в области координации политики взаимодействия стран – членов Организации в рамках направлений ее деятельности, главным структурным органом Америпола, являющимся центром организации международного сотрудничества и принимающим основные решения, посредством которых достигаются цели Америпола, является Совет Директоров. В него входят главы и руководители полицейских служб стран – участниц Америпола. Все решения Совета Директоров утверждаются Исполнительным Секретариатом.

Исполнительный Секретариат – это постоянный исполнительный орган Америпола, осуществляющий функции по обеспечению эффективной работы Организации, в том числе методическими, организационными, техническими средствами. Секретариат избирается сроком на три года. Если роспуск Секретариата совпадает с датой отставки Генерального Секретаря, то срок полномочий Секретариата увеличивается до четырех лет.

В ближайшее время не исключается возможность появления новых организаций такого рода. В частности, многие ученые на страницах научных периодических изданий уже размышляют о возможностях учреждения Евразпола – Евразийской полиции, которая могла бы усилить борьбу с преступностью. При этом стоит отметить, что Евразпол не является единственной перспективной международной региональной полицейской организацией.

В свою очередь, деятельность НЦБ Интерпола России основывается на Уставе Международной организации уголовной полиции (Интерпол), решениях ее Генеральной Ассамблеи, а также ведомственных нормативных правовых актах. Основной ведомственный нормативный правовой акт, которым руководствуются территориальные органы внутренних дел при необходимости получения информации в системе Интерпола, – это Инструкция об организации информационного обеспечения сотрудничества по линии Интерпола[138]. При этом важно отметить, что данный документ периодически обновляется, а до него действовал аналогичный документ 2000 г., который приказом от 06.10.2006 признан утратившим силу.

В сфере обеспечения кибербезопасности Интерпол осуществляет международное сотрудничество по таким вопросам, как оперативная и следственная поддержка, кибернетическая разведка и анализ, цифровая

[138] Об утверждении Инструкции по организации информационного обеспечения сотрудничества по линии Интерпола : приказ МВД России № 786, Минюста России № 310, ФСБ России № 470, ФСО России № 454, ФСКН России № 333, ФТС России № 971 от 6 октября 2006 года : с изм. на 22 сентября 2009 года // Кодекс: Электронный фонд правовых и нормативно-технических документов : сайт. URL: https://docs.cntd.ru/document/902011678?ysclid=lmdccjb898964362998 (дата обращения: 21.03.2023).

криминалистика, инновации и исследования, наращивание технического и научного потенциала, национальные киберобзоры[139].

Наше государство очень заинтересовано в эффективном взаимодействии с другими странами в целях борьбы с преступностью (во всех ее проявлениях, начиная от коррупции и заканчивая международными актами терроризма). Подчеркнем, что в настоящий период практически во всех видах преступности прослеживается тенденция использования тех или иных цифровых технологий, будь то финансирование терроризма, подкуп государственных служащих и т. д. Именно поэтому международное полицейское сотрудничество в вопросах противодействия цифровым преступлениям так или иначе строится на взаимодействии в борьбе со всеми остальными видами преступности. Эти аспекты очень тесно взаимосвязаны между собой. Проявляется это, в частности, в том, что представители МВД России совместно с иными властными субъектами приняли (и при этом регулярно обновляют) нормативный правовой акт (Инструкцию), направленный на регулирование вопросов взаимодействия сотрудников оперативных подразделений России с представителями оперативных подразделений иных стран. В этой связи очень важно продолжать вести совместную международную работу по борьбе с таким негативным социальным явлением, как преступность, в том числе в цифровой сфере.

Задачей Интерпола является организация взаимодействия всех правоохранительных органов мира, то есть в Российской Федерации представительство Интерпола является органом межведомственного взаимодействия и может получать запросы от зарубежных стран, взаимодействовать со всеми ведомствами нашего государства, а по некоторым вопросам – даже с государственными органами, если это касается розыска лиц, похищенных культурных ценностей или автотранспортных средств.

Международная деятельность правоохранительных органов нашего государства направлена не только на борьбу с выводом денег за рубеж, но и на экстрадицию преступников, поиск пропавших и защиту интересов иностранцев в разных государствах. Интерпол помогает решать международные политические коллизии.

Киберпреступность справедливо признается одним из наиболее опасных современных асоциальных явлений, поскольку ее деятельность направлена на проникновение в различные сферы социально-экономической и политической общественной жизни. Преступная кибердеятельность угрожает мировому сообществу, именно поэтому перед многими государствами мира стоит задача борьбы с цифровой

[139] Ситков, А. С. Международное сотрудничество полиции в рамках Интерпола по противодействию киберпреступности и обеспечению кибербезопасности // Вестник Московского университета МВД России : науч. журн. 2022. № 5. С. 240.

преступностью. И учитывая трансграничный характер цифровой преступности, мы понимаем, что такая борьба не может вестись в одиночку, в данном вопросе требуется взаимодействие разных государств.

На наш взгляд, оптимальным решением является разработка и принятие между странами рамочного соглашения по регулированию деятельности ОВД. На подобный механизм также обращают внимание современные исследователи[140]. И как мы уже говорили, цифровая преступность нередко проявляется в террористических формах (например, при финансировании террористических организаций). Деятельность террористических объединений отличается направленностью на то, чтобы обеспечить приспособление и преобразование общественных условий в собственных целях. Следует признать, что чаще всего они добиваются этого. Вероятно, основными причинами этого выступают просчеты государств и неготовность социума к противодействию терроризму. В связи с этим следует говорить о необходимости проведения грамотной борьбы государства с данным асоциальным явлением и особой осведомленности населения при столкновении с такой преступной деятельностью. Именно поэтому важно не просто развивать, но и совершенствовать механизм международного полицейского сотрудничества, в том числе в целях противодействия цифровому финансированию терроризма. Необходимо, в частности, совершенствовать законодательную базу, регламентирующую борьбу с террористами, определяющую ответственность за их преступные деяния.

Еще один аспект международного полицейского сотрудничества в вопросах борьбы с цифровыми преступлениями связан с необходимостью согласования уголовных политик разных стран. Иными словами, речь идет о том, что каждое государство реализует собственную уголовную политику. Она может проявляться в преобразовании и совершенствовании работы подразделений тех или иных правоохранительных органов. Однако проблема заключается в том, что уголовная политика разных стран может не совпадать. А это значит, что появляется необходимость в международном согласовании таких политик.

При этом вопросы государственной (в том числе уголовной) правовой политики активно рассматривались в юридических науках еще в XIX веке. Деятельность Франца фон Листа, руководителя Социологической школы уголовного правосудия, в частности его работа «Задачи в области уголовной политики», оказала значительное влияние на убеждения отечественных юристов в этой области. В своей работе Франц фон Лист писал, что уголовная политика представляет собой

[140] Тузов, Л. Л., Шейшеев, А. Д. Сотрудничество оперативных подразделений ОВД на международном уровне в противодействии организованной преступности и коррупции // Вестник Московского университета МВД России : науч. журн. 2013. № 4. С. 133.

систематический сборник этих основных положений, соглашаясь с тем, что государство должно бороться с преступностью с помощью наказания и родственных ему установлений. И борьба с цифровой преступностью в данном случае не исключение. Процессы демократических перемен в российском обществе показали острую необходимость разработки стратегии развития страны не только в социально-экономической, но и в правовой сфере.

Подводя небольшой итог, можно отметить следующее.

Во-первых, международное взаимодействие подразделений ОВД в борьбе с цифровой преступностью развивалось и развивается в целом в рамках института международного содействия в борьбе с преступностью. Первые зачатки международного сотрудничества по указанным вопросам можно найти еще в древности, когда правители разных стран пытались совместными усилиями бороться с бегством рабов, с пиратством в открытом море и т. д.

Во-вторых, с развитием общественных отношений, с развитием государств меняются и формы взаимодействия тех или иных субъектов международного сотрудничества. Сейчас такое взаимодействие осуществляется на основании межгосударственных договоров, соглашений, конвенций и т. п. Большое значение в таком взаимодействии имеет ООН. Например, в целях укрепления и усиления деятельности, направленной на борьбу с финансированием терроризма посредством использования современных цифровых технологий, различные дружественные государства начали в сентябре 2006 г. новый этап борьбы с терроризмом, приняв глобальную контртеррористическую стратегию. И в реализации указанной стратегии немаловажная роль отводится именно подразделениям полиции разных государств.

В-третьих, международное полицейское сотрудничество, пройдя длительный пусть становления и изменения, в настоящий период играет важную роль в вопросах предупреждения современной цифровой преступности. В этой связи можно еще раз сделать вывод об актуальности данного пособия.

ЗАКЛЮЧЕНИЕ

В завершение изучения темы, связанной с особенностями квалификации и предупреждения преступлений, совершаемых с использованием информационных (цифровых) технологий, необходимо отметить следующее.

В современных реалиях защита цифрового пространства является одной из актуальных задач государственных и правоохранительных структур. Развитие современных технологий не останавливается. Новые общественные отношения в данной области возникают столь стремительно, что нормативно-правовое регулирование не успевает за этими процессами. При этом Российская Федерация столкнулась с цифровой преступностью только в 90-е годы XX века. В связи с тем, что цифровая преступность (киберпреступность) выделяется в самостоятельный вид преступной деятельности, возможны детальное изучение ее особенностей, специфики детерминации, причинности, а также выработка дифференцированных мер по борьбе с ней.

В связи с актуальностью и распространенностью цифровых отношений, а также проблем, возникающих с их появлением и развитием, достаточно большое количество исследователей уже обратились к изучению обозначенной проблематики. Это, например, В. М. Быков, О. С. Гузеева, О. С. Капинус, В. В. Крылов, Е. А. Русскевич, А. В. Суслопаров, Л. Г. Устьев, В. Н. Черкасов, А. Е. Шарков, Н. А. Швед и многие другие исследователи.

Объектом нашего пособия выступили цифровые преступления, цифровая преступность, ее виды и криминологические особенности, а также особенности и способы борьбы с ней.

Подчеркнем, что пособие опирается на действующие нормативные правовые акты, регламентирующие ответственность за цифровые преступления, а также на материалы судебной практики. Осуществлен комплексный научный анализ понятия и общей характеристики цифровых преступлений в России, освещены ключевые уголовно-правовые и иные меры по их предупреждению и методы борьбы с ними.

Настоящее учебное пособие решило следующие научно-исследовательские задачи:

1) изучены современные подходы к определению цифровых преступлений;

2) проанализированы виды цифровых преступлений;

3) дана характеристика личностей киберпреступника и его жертвы;

4) выявлены меры по предупреждению киберпреступлений;

5) рассмотрены актуальные проблемы борьбы с цифровыми преступлениями, возникающие при осуществлении международного сотрудничества в вопросах противодействия цифровой преступности.

Коротко отметим, что в общем смысле под киберпреступлением (или цифровым преступлением) подразумевается любое виновное общественно опасное посягательство, совершенное за счет использования ИТ-технологий или в самом информационном пространстве.

В то же время информационными технологиями именуются как технические устройства с выходом в сеть Интернет, к числу которых следует отнести персональные компьютеры, ноутбуки, гаджеты, так и сама информация с ее материальными носителями[141].

Необходимо понимать, что цифровые преступления всегда взаимодействуют с информационным пространством. Информационное пространство – это прежде всего информационно-телекоммуникационная сеть. Например, к таковым стоит отнести сеть Интернет, локальную компьютерную сеть и т. д. При этом главной особенностью совершения вышеуказанной разновидности противоправных посягательств является место совершения уголовно наказуемого деяния.

Среди факторов, способствующих совершению цифровых преступлений, следует отметить высокий уровень правового нигилизма в нашем государстве. Большинство граждан не знают о том, какие именно преступления следует относить к цифровым и как вести себя, чтобы не стать жертвой киберпреступника.

Как мы уже отмечали, судебная практика и статистика по делам о цифровых преступлениях на современном этапе достаточно разнообразна, и, к сожалению, пока не выработаны единые подходы к квалификации преступлений в данной сфере, что предполагает необходимость внесения отдельных законодательных изменений либо урегулирования спорных вопросов в актах Верховного Суда Российской Федерации.

Настоящее учебное пособие имеет практическое назначение, которое заключается в том, что представленные в нем выводы и результаты:

1) могут использоваться в дальнейшем в учебном процессе по таким дисциплинам и отраслям права, как:

– «Информационное право»;

– «Правовые вопросы функционирования информационных систем»;

– «Правозащитная деятельность и права человека» и пр.

2) могут выступить в качестве учебного материала для разработки курсовых, выпускных квалификационных и диссертационных работ, а также контрольных работ.

---

[141] Буз, С. И. Киберпреступления: понятие, сущность и общая характеристика // Юристъ-Правоведъ : науч. журн. 2019. № 4 (91). С. 82.

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

Нормативные правовые акты

1. Российская Федерация. Законы. Уголовный кодекс Российской Федерации : УК : принят Государственной Думой 24 мая 1996 года : одобрен Советом Федерации 5 июня 1996 года : последняя редакция // КонсультантПлюс : сайт. – URL: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 21.06.2023).

2. Российская Федерация. Законы. О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации : Федеральный закон № 259-ФЗ : принят Государственной Думой 22 июля 2020 года : одобрен Советом Федерации 24 июля 2020 года : последняя редакция // КонсультантПлюс : сайт. – URL: https://www.consultant.ru/document/cons_doc_LAW_358753/ (дата обращения: 21.06.2023).

3. Российская Федерация. Законы. Об информации, информационных технологиях и о защите информации : Федеральный закон № 149-ФЗ : принят Государственной Думой 8 июля 2006 года : одобрен Советом Федерации 14 июля 2006 года : последняя редакция // КонсультантПлюс : сайт. – URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 21.06.2023).

4. Российская Федерация. Верховный Суд. О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» : Постановление Пленума Верховного Суда Российской Федерации от 15 декабря 2022 года № 37 // КонсультантПлюс : сайт. – URL: https://www.consultant.ru/document/cons_doc_LAW_434573/?ysclid=lm8vfb22at602297918 (дата обращения: 21.06.2023).

Специальная литература

1. Бойко, О. А. Детерминанты латентных преступлений, совершаемых с использованием информационно-телекоммуникационных технологий / О. А. Бойко, А. С. Унукович // Юридический вестник Самарского университета : научный журнал. – 2020. – № 6 (3). – С. 53–59.
2. Иванова, Л. В. Виды киберпреступлений по российскому уголовному законодательству / Л. В. Иванова // Юридические исследования : научный журнал. – 2019. – № 1. – С. 25–33.
3. Ищук, Я. Г. Цифровая криминология : учебное пособие / Я. Г. Ищук, Т. В. Пинкевич, Е. С. Смольянинов. – Москва : Академия управления МВД России, 2021. – 244 с.
4. Маслиенко, М. А. Киберпреступность на современном этапе / М. А. Маслиенко // Проблемы правоохранительной деятельности : научный журнал. – 2021. – № 2. – С. 28–32.
5. Машевская, О. В. Цифровые технологии как основа цифровой трансформации современного общества / О. В. Машевская // Вестник Полесского государственного университета. Серия общественных и гуманитарных наук : научный журнал. – 2020. – № 1. – С. 37–44.
6. Поляков, И. В. Цифровая преступность: проблемы понятийного аппарата, систематизации и правоприменительной практики / И. В. Поляков // Проблемы правоохранительной деятельности : научный журнал. – 2020. – № 4. – С. 21–25.
7. Прокопенко, А. Н. Основные направления международного сотрудничества России в области противодействия преступности в социальных сетях / А. Н. Прокопенко, И. Н. Старостенко // Проблемы правоохранительной деятельности : научный журнал. – 2018. – № 4. – С. 53–59.
8. Сидорова, Е. З. Обеспечение криминологической безопасности в организациях общего и среднего профессионального образования : специальность 12.00.08 «Уголовное право и криминология; уголовно-исполнительное право» : автореферат диссертации на соискание ученой степени кандидата юридических наук / Сидорова Екатерина Закариевна ; Российская академия адвокатуры и нотариата. – Москва, 2018. – 29 с.
9. Сидорова, Е. З. Предупреждение преступлений и административных правонарушений органами внутренних дел : учебное пособие / Е. З. Сидорова, О. П. Грибунов. – Иркутск : Восточно-Сибирский институт МВД России, 2023. – 132 с.
10. Сидорова, Е. З. Примерный прогноз развития криминальной ситуации на объектах транспортной инфраструктуры Восточно-Сибирской железной дороги / Е. З. Сидорова // Социально-экономический и гуманитарный журнал : научный журнал – 2022. – № 3 (25). – С. 155–173.

11. Сидорова, Е. З. Принципы и значение уголовной политики в сфере предупреждения преступности в образовательной среде / Е. З. Сидорова // Сибирское юридическое обозрение : научный журнал. – 2021. – Т. 18. – № 4. – С. 423–432.

12. Сидорова, Е. З. Уголовно-правовое противодействие финансированию экстремистской деятельности и терроризма : монография / Е. З. Сидорова. – Иркутск : Восточно-Сибирский институт МВД России, 2023. – 96 с.

13. Сидорова, Е. З. Уголовная политика в сфере образования / Е. З. Сидорова, С. С. Босхолов // Академический юридический журнал : научный журнал – 2021. – Т. 22. – № 3 (85). – С. 253–259.

14. Токтарова, В. И. Цифровая грамотность: понятие, компоненты и оценка / В. И. Токтарова, О. В. Ребко // Вестник Марийского государственного университета : научный журнал. – 2021. – Т. 15. – № 2 (42). – С. 165–177.

15. Уголовное право Российской Федерации. Особенная часть : учебник / под ред. проф. М. В. Бавсуна ; 2-е изд., перераб. и доп. – Омск : Омская академия МВД России, 2020. – 768 с.

16. Ульянов, М. В. Преступления, совершаемые с использованием информационных технологий: динамика и тенденции / М. В. Ульянов // Общество и право : научный журнал. – 2020. – № 2 (72). – С. 32–36.

Учебное издание

Сидорова Екатерина Закариевна
Грибунов Олег Павлович

ОСОБЕННОСТИ КВАЛИФИКАЦИИ И ПРЕДУПРЕЖДЕНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ (ЦИФРОВЫХ) ТЕХНОЛОГИЙ

Учебное пособие

Редактор
Л. Ю. Ковальская

Подписано в печать 06.02.2024. Формат 60 х 84/16
Усл. печ. л. 8,0. Тираж 100 экз. Заказ № 2.

Восточно-Сибирский институт МВД России,
г. Иркутск, ул. Лермонтова, 110.
Отпечатано в НИиРИО Восточно-Сибирского института МВД России,
г. Иркутск, ул. Лермонтова, 110.