МГЮА

приоритет2030^
право для лидерства

ОБЗОР

правоприменительной практики по противодействию киберпреступлений

КИБЕРПРАВО

СПИСОК ИСПОЛНИТЕЛЕЙ

Заведующий кафедрой
криминологии и уголовно-исполнительного права,
доктор юридических наук, профессор Е.А. Антонян

Заведующий кафедрой
криминологии и уголовно-исполнительного права,
доктор юридических наук, профессор Е.Р. Россинская

Профессор кафедры
криминологии и уголовно-исполнительного права,
доктор юридических наук, профессор Е.Н. Клещина

Старший преподаватель кафедры
криминологии и уголовно-исполнительного права,
кандидат юридических наук Е.А. Братцева

Преподаватель кафедры
криминологии и уголовно-исполнительного права,
кандидат юридических наук И.С. Мочалкина

Оглавление

1. Понятие, состояние и тенденции киберпреступности в Российской Федерации

Являясь отдельным видом преступности, под киберпреступностью следует понимать социально-правовое, исторически изменчивое, негативное, массовое явление, представляющее собой совокупность киберпреступлений, совершенных лицами на определенной территории в определенный период времени, обладающее количественными и качественными показателями[1]. Однако на законодательном уровне в России понятия киберпреступления не закреплено, что порождает трудность в установлении указанной выше совокупности и обуславливает необходимость установления перечня составов преступлений, подпадающих под киберпреступления.

Одним из первых шагов в определении круга преступлений, являющихся киберпреступлениями, можно считать принятие в ноябре 2001 года в Будапеште Европейской Конвенции по киберпреступлениям (англ. – Convention on Cybercrime) или так называемой Конвенции о преступности в сфере компьютерной информации[2], в которой приводится классификация киберпреступлений. Так, в указанном документе рекомендуется квалифицировать в качестве преступлений согласно внутригосударственному праву следующие деяния:

1. Преступления против конфиденциальности, целостности и доступности компьютерных данных и систем (противозаконный доступ, неправомерный перехват, воздействие на данные, воздействие на функционирование системы, противозаконное использование устройств);

2. Правонарушения, связанные с использованием компьютерных средств (подлог с использованием компьютерных технологий, мошенничество с использованием компьютерных технологий);

3. Правонарушения, связанные с содержанием данных (правонарушения, связанные с детской порнографией);

[1] Криминология: учебник / отв. ред. В.Е. Эминов. – Москва : Проспект, 2023. – С. 29.
[2] Конвенция по киберпреступлениям. URL: https://base.garant.ru/4089723/ (дата обращения: 15.07.2023).

4. Правонарушения, связанные с нарушением авторского права и смежных прав.

Стоит отметить, что Россия не подписала рассмотренную выше Конвенцию по киберпреступлениям, следовательно, ее положения не могут быть признаны частью правовой системы нашей страны. Вместе с тем, согласно данным официального сайта Прокуратуры Карачаево-Черкесской Республики РФ, киберпреступностью является любая преступная активность, где объектом в качестве цели и/или инструмента является компьютер или сетевое устройство[3]. При этом разделить киберпреступления на отдельные категории не так просто, однако в целом можно выделить следующие виды:

1. Финансово-ориентированные киберпреступления (фишинг, кибервымогательство, финансовое мошенничество);

2. Киберпреступления, связанные с вторжением в личную жизнь (кража персональных данных, шпионаж);

3. Нарушение авторского права.

Согласно статистическим данным Отчета МВД РФ ФКУ «Главный информационно-аналитический центр» по состоянию преступности[4] в России за январь-декабрь 2022 года (*далее – Отчет МВД РФ 2022*), всего в указанном отчетном периоде было зарегистрировано 1966795 преступлений, из которых 522065 преступлений совершены с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации[5]. Среди преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, в Отчете МВД РФ 2022 указываются следующие преступления:

---

[3] Официальный сайт Прокуратуры Карачаево-Черкесской Республики. URL: https://epp.genproc.gov.ru/ru/web/proc_09/activity/legal-education/explain?item=63269279 (дата обращения: 15.07.2023).

[4] Состояние преступности определяется общим количеством преступлений и лиц, их совершивших, на определенной территории в определенный период времени. Всегда выражается абсолютным числом. Криминология: учебник / отв. ред. В.Е. Эминов. – Москва : Проспект, 2023. – С. 34.

[5] Отчет МВД РФ ФКУ «Главный информационно-аналитический центр» по состоянию преступности в России 2022. URL: https://мвд.рф/reports/item/35396677/ (дата обращения: 08.07.2023).

- кража (ст. 158 УК РФ) – 113565;

- мошенничество (ст. 159 УК РФ) – 249984;

- мошенничество с использованием электронных средств платежа (ст. 159^3 УК РФ) – 7288;

- мошенничество в сфере компьютерной информации (ст. 159^6 УК РФ) – 334;

- незаконные организация и проведение азартных игр (ст. 171^2 УК РФ) – 583;

- публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма (ст. 205^2 УК РФ) – 490;

- 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) – 62209;

- изготовление порнографических материалов (ст. 242, 242^1, 242^2 УК РФ) – 2588;

- публичные призывы к осуществлению экстремистской деятельности (ст. 280 УК РФ) – 493;

- преступления в сфере компьютерной информации (глава 28 УК РФ) – 10027.

Стоит отметить, что из числа преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, раскрыты только 142384 преступления; при этом выявлено 96665 лиц, совершивших данные преступления.

Исходя из Отчета МВД РФ 2022 можно сделать вывод не только о состоянии преступности в РФ, но и о ее тенденциях. Так, с использованием высоких технологий было совершено каждое четвертое преступление, при этом зарегистрировано на 27,6% меньше краж, на 29% – фактов мошенничества с использованием электронных средств платежа, на 22,5% –

криминальных деяний в сфере компьютерной информации. Правоохранительными органами больше на 20,9% зарегистрировано фактов сбыта наркотиков. Кроме того, увеличилось количество заведомо ложных сообщений об акте терроризма, в массиве которых 92,2% совершены дистанционно. Раскрываемость преступлений, совершенных с использованием IT-технологий, возросла на 4,4%[6].

Согласно статистическим данным Отчета МВД РФ ФКУ «Главный информационно-аналитический центр» по состоянию преступности в России за январь-май 2023 года (*далее – Отчет МВД РФ 2023*), всего в указанном отчетном периоде было зарегистрировано 813852 преступлений, из которых 261049 преступлений совершены с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации[7]. Среди преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, в Отчете МВД РФ 2023 указываются следующие преступления:

- кража (ст. 158 УК РФ) – 46434;

- мошенничество (ст. 159 УК РФ) – 134742;

- мошенничество с использованием электронных средств платежа (ст. 159^3 УК РФ) – 2459;

- мошенничество в сфере компьютерной информации (ст. 159^6 УК РФ) – 243;

- незаконные организация и проведение азартных игр (ст. 171^2 УК РФ) – 286;

- публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма (ст. 205^2 УК РФ) – 244;

[6] Там же.

[7] Отчет МВД РФ ФКУ «Главный информационно-аналитический центр» по состоянию преступности в России 2023. URL: https://мвд.рф/reports/item/39336121/ (дата обращения: 08.07.2023).

- 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) – 35232;

- изготовление порнографических материалов (ст. 242, 242^1, 242^2 УК РФ) – 1069;

- публичные призывы к осуществлению экстремистской деятельности (ст. 280 УК РФ) – 198;

- преступления в сфере компьютерной информации (глава 28 УК РФ) – 9181.

Стоит отметить, что из числа преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, раскрыты только 71370 преступлений; при этом выявлено 44357 лиц, совершивших преступления.

Исходя из Отчета МВД РФ 2023 можно сделать вывод, что зарегистрирован рост числа преступлений, совершенных с использованием информационно-телекоммуникационных технологий на 27,5%. Вместе с тем, меньше на 31,8% стало мошенничеств с использованием электронных средств платежа, а количество IT-краж осталось на уровне прошлого года[8].

Таким образом, представляется, что из-за отсутствия в законодательстве РФ дефиниции киберпреступления, сложно определить полный перечень преступлений, закрепленных в УК РФ, подпадающих под рассматриваемое понятие. В силу того, что в Отчетах МВД РФ о состоянии преступности указан перечень преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, который по своему содержанию в определенной части пересекается с рекомендациями Конвенции по киберпреступлениям, Прокуратуры РФ, в дальнейшем тексте настоящего исследования под

[8] МВД России публикует статистическую информацию о состоянии преступности в Российской Федерации за пять месяцев 2023 года. URL: https://мвд.рф/news/item/39322163 (дата обращения: 08.07.2023).

киберпреступлениями предлагается понимать те составы преступлений, закрепленные в рассмотренных выше отчетах.

2. Детерминирующее влияние информационно-коммуникационных технологий на формирование способов совершения преступлений на современном этапе

Новые информационно-коммуникационные технологии (ИКТ), масштабно внедряемые в жизнь современного общества, ожидаемо оказались широко востребованными преступным сообществом, что, наряду с другими факторами, напрямую либо косвенно связанными с цифровизацией всех сторон жизни человека, общества и государства, привело к появлению такого негативного социального феномена как киберпреступность, а также к тому, что такие понятия как «киберпреступление» либо «компьютерное преступление» вошли в массовое употребление.

Надо признать, упомянутые термины являются дискуссионными, не имеют четких и устоявшихся дефиниций, а их содержание зачастую зависит от национальных законодательств и международных правовых актов, в которых они упоминаются.

Но основная тенденция в толковании прослеживается достаточно отчетливо - данными понятиями охватываются не только киберзависимые преступления, то есть те, которые могут быть совершены исключительно с использованием ИКТ[9], но и традиционные преступления, при совершении которых также используются компьютерные системы.

Компьютерные преступления имеют общую родовую криминалистическую характеристику, включающую сведения о способах преступлений, лицах, совершивших их, сведения о потерпевшей стороне и обстоятельствах, способствующих и препятствующих данным

[9] McGuire and Dowling. Cyber crime: A reviewof the evidence. Research Report 75. Chapter 2: Cyber-enabled crimes-fraud and theft // [Электронный ресурс]. - Режим доступа: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/248621/horr75-chap2.pdf (дата обращения 20.11.2022).

преступлениям[10]. В этой связи дефиниция «компьютерное преступление» должна употребляться не в уголовно-правовом аспекте, где это только затрудняет квалификацию деяния, а в криминалистическом, поскольку связана не с квалификацией, а именно со способом преступления и, соответственно, с методикой его раскрытия и расследования.

В этом смысле к компьютерным отнесем не только преступления, объектом которых выступают общественные отношения в сфере обработки, хранения и передачи компьютерной информации (т.н. киберзависимые преступления), а любые преступные посягательства, совершаемые с применением ИКТ, или, если использовать недавно приведенный в законе термин, - преступления в сфере информационных технологий[11].

Компьютерная информация применительно к процессу доказывания может быть определена как фактические данные, обработанные компьютерной системой и (или) передающиеся по телекоммуникационным каналам, а также доступные для восприятия, на основе которых в определенном законом порядке устанавливаются обстоятельства, имеющие значение для правильного разрешения уголовного, гражданского или административного дела[12].

Для исследования закономерностей возникновения и движения криминалистически значимой компьютерной информации обратимся к криминалистической дефиниции механизма преступления, который представляет собой сложную динамическую систему, определяющая содержание преступной деятельности. Элементами механизма преступления являются: субъекты преступления; отношение субъекта преступления к

---

[10] Россинская Е.Р. Криминалистика. Учебник для вузов. – М.: Норма-ИНФРА-М, 2016. С. 440–442; Аверьянова Т.В., Белкин Р.С., Корухов Ю.Г., Россинская Е.Р. Криминалистика. Учебник для вузов. Изд. 4 переработанное и доп. – М.: Норма-ИНФРА-М, 2014. С.903–905.

[11] «О ратификации Соглашения о сотрудничестве государств — участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий». [Электронный ресурс]. - Режим доступа: https://www.pnp.ru/law/2021/07/01/federalnyy-zakon-237-fz.html (дата обращения - 20.11.2021).

[12] Аверьянова Т.В., Белкин Р.С., Корухов Ю.Г., Россинская Е.Р. Криминалистика. Учебник для вузов. Изд. 4 переработанное и доп./ Т.В. Аверьянова, Р.С. Белкин, Ю.Г. Корухов, Е.Р. Россинская. – М.: Норма-ИНФРА-М, 2014. С. 904.

своим действиям, их последствиям, соучастникам; предмет посягательства; способ преступления; преступный результат; обстановка преступления (место, время и другие относящиеся к ней обстоятельства); поведение и действия лиц, оказавшихся случайными участниками события, и др.[13] Одним из важнейших элементов механизма преступления является способ преступления.

Способ преступления по классическому определению Зуйкова Г.Г. «представляет собой систему объединённых единым замыслом действий преступника (преступников) по подготовке, совершению и сокрытию преступления, детерминированных объективными и субъективными факторами, действий, сопряженных с использованием соответствующих орудий и средств»[14]. Другими словами, способ преступления – это детерминированная личностью, предметом и обстоятельствами преступного посягательства система действий субъекта, направленная на достижение преступной цели и объединенная единым преступным замыслом. В этой системе могут быть выделены действия по подготовке, совершению и сокрытию следов преступления[15]. В зависимости от этого способы преступления делят на полноструктурные и неполноструктурные. Полноструктурный способ включает действия, относящиеся ко всем его элементам: подготовке, совершению и сокрытию. В тех случаях, когда преступление совершается без предварительной подготовки или когда субъект преступления не планирует действий по его сокрытию, налицо

[13] Россинская Е.Р. Криминалистика. Учебник для вузов. – М.: Норма-ИНФРА-М, 2016. С.17; Криминалистика: учебник студентов для вузов / под ред. А.Ф. Волынского, В.П. Лаврова. – 2 изд., перераб. и доп. – М.: ЮНИТИ-ДАНА: Закон и право, 2008. С. 27.

[14] Зуйков Г.Г. Криминалистическое учение о способе совершения преступления: автореф. дис. ... д-ра юрид. наук. – М.: Высш. школа МВД СССР, 1970. С. 10; Зуйков Г.Г. Основы криминалистического учения о способе совершения и сокрытия преступления. Гл.3. В Криминалистика. Учебник для юридических вузов МВД СССР / Под ред. Р.С. Белкина, В.П. Лаврова, И.М. Лузгина. – М. Академия МВД СССР, 1987, т. 1. С.52.

[15] Аверьянова Т.В., Белкин Р.С., Корухов Ю.Г., Россинская Е.Р. Криминалистика. Учебник для вузов. Изд. 4 переработанное и доп. –. М.: Норма-ИНФРА-М, 2014. С. 62.

неполноструктурный способ совершения преступления. При этом возможно формирование самостоятельного способа сокрытия преступления[16].

Как отмечал Белкин Р.С., способ преступления, понимаемый как система действий преступника по подготовке, совершению и сокрытию преступления, будучи в целом отражаемым объектом, как элемент объективной стороны преступления, в то же время своими составляющими (действия, средства действий) служит средством отражения в среде события преступления[17]. Кроме того, «следы определенного способа совершения преступления указывают не только на совершенные действия, но и на обстоятельства, детерминировавшие способ совершения преступления, определившие состав и характер совершенных действий, в частности, по характеру совершенных действий представляется возможным предположительно судить об определивших способ совершения преступления качествах личности»[18].

На формирование способа преступления оказывают влияние объективные и субъективные факторы, что определяет детерминированность и повторяемость способов преступления. Зуйков Г.Г. отмечает, что «абсолютная повторяемость способов преступлений во всех их признаках полностью исключена. Способы преступлений повторяются, если сохраняется действие определенных факторов, их детерминирующих (мотив и цель преступления, объективная обстановка его совершения, качества личности преступника, особенности предмета преступного посягательства и т.д.), а так как детерминирующие факторы изменяются и в количественном и в качественном отношениях, то неизбежно изменяются и способы совершения преступлений, сохраняя, однако, некоторую совокупность повторяющихся признаков»[19].

---

[16] Зуйков Г.Г. Основы криминалистического учения о способе совершения и сокрытия преступления. Гл.3. В Криминалистика. Учебник для юридических вузов МВД СССР / Под ред. Р.С. Белкина, В.П. Лаврова, И.М. Лузгина. – М. Академия МВД СССР, 1987, т. 1. С.50-51.

[17] Белкин Р.Р. Курс криминалистики. 3 изд. дополненное. – М.: ЮНИТИ-ДАНА, Закон и Право, 2001. С.71.

[18] Зуйков Г.Г. Криминалистическое учение о способе совершения преступления. Гл.6. В кн.: Криминалистика. / Под ред. Р.С. Белкина, И.М. Лузгина. – М. Академия МВД СССР, 1978, т. 1. С.60.

[19] Зуйков Г.Г. «Модус операнди», кибернетика, поиск // Кибернетика и право, 1970. С.50.

Как отмечает Чулахов В.Н., среди факторов, определяющих способ преступления, значительную роль играют психофизиологические свойства личности преступника, в частности навыки и привычки. В способе преступления отражаются два вида навыков – общего значения, возникшие вне связи с совершением преступления, и преступные, сформированные в процессе противоправной деятельности. Навыки преступного характера формируются в ходе подготовки к преступлению и совершенствуются при повторных аналогичных преступлениях[20]. Превращение некоторых самостоятельных элементов способа в навык и переход их на уровень автоматизированных, подсознательных актов является одной из закономерностей формирования способа неоднократно совершаемых однородных преступлений, т.е. формируется «преступный почерк».

3.Способы совершения киберпреступлений

Способы совершения киберзависимых компьютерных преступлений

Описание способов компьютерных преступлений начнем с действий по сокрытию преступниками своих данных при использовании сети Интернет с целью предотвращения идентификации их личности. Для сокрытия своего адреса преступники используют различные анонимные компьютерные сети и сервисы, специально созданные для этих целей.

Одним из таких способов является использование VPN-сервисов (англ. Virtual Private Network — виртуальная частная сеть)[21]. Технологии VPN обеспечивают шифрование сетевого трафика между компьютером пользователя и VPN-прокси-сервером, который является шлюзом выхода в сеть Интернет и, соответственно, скрывает реальный IP-адрес пользователя. Если им требуется высокий уровень конспирации, преступники арендуют у провайдеров хостинговых услуг вычислительные мощности практически в любой точке мира, на которых настраивают собственные VPN-серверы либо

[20] Чулахов В.Н. Криминалистическое учение о навыках и привычках человека: монография / под ред. Е. Р. Россинской. – М.: Юрлитинформ. С.206-207.
[21] Куроуз Д., Росс К. Компьютерные сети: нисходящий подход. 6 изд. - М., 2016. С. 794-795.

виртуальные машины, с которых, используя сторонние VPN-сервисы, выходят в сеть Интернет.

Другой способ, использование которого позволяет скрыть свой IP-адрес, – The Onion Routing, TOR (луковая маршрутизация второго поколения) – технология и программное обеспечение для реализации обмена данными с многослойным шифрованием с помощью системы прокси-серверов, обеспечивающих анонимное сетевое подключение[22].

Троянская программа, обладающая функциональными возможностями VPN-прокси-сервера, также позволяет преступникам создать бот-сеть из компьютеров, зараженных такой программой, и использовать ее для сокрытия своего IP-адреса.

Помимо упомянутых способов анонимизации своих действий в сети Интернет путем построения цепочки прокси-серверов преступники для этих целей применяют и другие криминальные либо полукриминальные схемы, например, через несанкционированное подключение к сторонним беспроводным точкам доступа – Wi-Fi роутерам, либо с помощью беспроводных модемов мобильной связи с SIM-картами, оформленными на посторонних лиц.

Выбор безопасных способов оплаты сервисов и вычислительных мощностей для осуществления преступной деятельности также является мерой конспирации преступной деятельности. Для этих целей широко используется так называемая криптовалюта, например, биткоины, правовой режим которой во многих странах мира, в том числе в России, остается неопределенным.

Разработка планов преступной деятельности, координация мероприятий на стадии подготовки к совершению преступления, согласование совместных действий осуществляются соучастниками с применением сетевых протоколов обмена сообщениями, обеспечивающих

[22] Ligh M., Adair S., Hartstein B., Richard M. Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code. - Indianapolis, 2010. P. 2-5

безопасность передачи данных. Одной из востребованных реализаций коммуникации в криминальной среде является XMPP-протокол (eXtensible Messaging and Presence Protocol) обмена мгновенными сообщениями, известный еще как Jabber-протокол (буквально – болтовня), который предоставляет возможность настроить свой собственный Jabber-сервер, обеспечивающий шифрование канала[23]. Вместе с тем в настоящее время широчайшее распространение в криминальной среде получили программы-мессенджеры, обеспечивающие стойкое шифрование между устройствами пользователей, так называемое end-to-end шифрование (Telegram, Signal, VIPole и др.).

К мерам по сокрытию следов преступления можно отнести также способы, с помощью которых преступники оказывают противодействие осмотру и изъятию компьютерной информации, содержащейся в их компьютерных средствах и системам, имеющей криминалистическое значение. Эти цели достигаются шифрованием компьютерных данных с помощью специализированного программного обеспечения либо возможностью быстрого уничтожения таких данных с использованием специальных программ или устройств.

Для сокрытия следов несанкционированного доступа и вредоносной активности на компьютере пользователя применяются различные меры технического характера, как прошедшие проверку временем технологии шифрования и обфускации (obfuscate — делать неочевидным, запутанным), так и новые приемы и методы.

Способы сокрытия вредоносной активности в системе:

- технологии Bootkit;
- технологии Rootkit;
- «бестелесная» технология;
- технологии криптования, обфускации и т.п.

[23] Торичко Р. С., Клишина Н. Е. Некоторые вопросы совершенствования действующего законодательства, регламентирующего расследование киберпреступлений // Вестник экономической безопасности. 2018. № 3. С. 181.

В процессе криптования исполняемый код вредоносной программы шифруется, а при обфускации приводится к виду, затрудняющему анализ и понимание алгоритмов его работы. Это осложняет выявление таких программ антивирусным программным обеспечением и их исследование специалистами информационной безопасности.

Вредоносные программы, функционирующие только в оперативной памяти компьютера и не сохраняющиеся на энергонезависимые запоминающие устройства, именуют «бестелесными». При отключении питания компьютера, например, при его перезагрузке, программа стирается. Такие программы применяются преступниками для сокрытия их активности от антивирусного программного обеспечения[24].

Технология Bootkit применяется для сокрытия вредоносного кода от антивирусного программного обеспечения и получения максимальных привилегий в системе. Для реализации этого способа вредоносной программой модифицируется, например, главная загрузочная запись (англ. master boot record, MBR), которая считывается процессором еще до начала загрузки операционной системы, а вредоносный код в зашифрованном виде записывается в неиспользуемую операционную систему область дискового пространства. При включении компьютера загрузчик еще до старта операционной системы расшифровывает и загружает в оперативную память вредоносный код[25]. Максимальные права пользователя позволяют применить набор программ Rootkit, которые скрывают вредоносную активность в системе: сетевые подключения, процессы, файлы и т.д.

Как видно из перечисленных мер, предпринимаемых преступниками с целью сокрытия следов несанкционированного доступа к компьютерным системам и информации пользователя, весьма значительное количество таких деяний совершается с помощью вредоносного программного

[24] Lenny Zeltser. The History of Fileless Malware – Looking Beyond the Buzzword. [Электронный ресурс]. - Режим доступа: https://zeltser.com/fileless-malware-beyond-buzzword (дата обращения - 20.11.2021).
[25] Matrosov A., Rodionov E., Bratus S. Rootkits and Bootkits: Reversing Modern Malware and Next Generation Threats. - No Starch Press, 2015. P. 504.

обеспечения. Преступники используют вредоносные программы для значительного усиления своих возможностей, то есть в криминалистическом плане вредоносная программа является орудием совершения преступления[26].

В уголовно-правовом смысле определение вредоносной программы изложено в ст. 273 УК РФ, согласно которой под вредоносной программой понимается компьютерная программа либо иная компьютерная информация, заведомо предназначенная для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации. К таким программам следует отнести не только специально разработанное, но и модифицированное легальное программное обеспечение, дополнительные функциональные возможности которого вследствие модификации наделяют его признаками вредоносности.

Заметим, что в качестве орудия совершения преступления может быть использована и легальная программа, функциональность которой предоставляет преступникам возможность достижения своих целей. Большинство легальных программ, используемых преступниками в противоправной деятельности, предназначены для удаленного несанкционированного доступа к компьютеру, управления системой и ее администрирования, например: RMS, Ammyy Admin, TeamViewer и LiteManager. Эти программы обладают функциональными возможностями, достаточными для достижения преступных целей, и определяются антивирусным программного обеспечения с менее критичным именем как условно-опасные, в связи с чем пользователи не видят в них особой угрозы. Кроме того, многие из этих программ являются доверенными программами пользователя, установлены с его ведома и не вызывают у него подозрений.

В последние годы особой популярностью у преступников, промышляющих получением несанкционированного доступа к

[26] Чекунов И.Г. Современные киберугрозы. Уголовно-правовая и криминологическая классификация и квалификация киберпреступлений // Право и кибербезопасность. 2012. № 1. С. 9-22.

компьютерным системам и информации, пользуется легальный программный инструментарий, предназначенный для проведения тестов на проникновение, например ПО CobaltStrike. В определенных случаях, например, когда необходимо отключить оповещение пользователя о работе программы либо ее модулей, такие программы подвергаются незначительной модификации, которая может привести к изменению их поведения (набора действий) в системе, которое будет соответствовать другому классу определяемых антивирусным программного обеспечения объектов – Malware (категории вредоносных программ).

Один из таких способов реализуется с помощью технологии DLL Hijacking[27], эксплуатирующей особенности функционирования операционной системы (ОС) Windows. Способ заключается в помещении в одну папку с файлом программы удаленного управления вредоносного библиотечного файла (dll-библиотеки), причем с таким же именем, что и расположенная в другой директории легальная библиотека. При запуске программа вместо легальной библиотеки загружает вредоносную, которая размещена «ближе». Например, для сокрытия от пользователя отображаемых на экране графических признаков работы программы TeamViewer (значка, окна сообщений) преступники осуществляют подмену библиотеки msvfw32.dll.

Самая общая классификация, широко применяемая в настоящее время для их систематизации, выделяет из класса вредоносных программ (Malware) следующие подклассы: программы-вирусы (Virus), программы-черви (Worm) и троянские программы (Trojan)[28].

К первым двум подклассам вредоносных программ относятся вирусы и черви, которые без ведома пользователя саморазмножаются на компьютерах и в компьютерных сетях, при этом каждая последующая копия также обладает способностью к саморазмножению.

---

[27] The MITRE Corporation. CWE-427: Uncontrolled Search Path Element. [Электронный ресурс]. - Режим доступа: https://cwe.mitre.org/data/definitions/427.html (дата обращения - 20.06.2023).

[28] Энциклопедия Лаборатории Касперского. Классификация детектируемых объектов. Вредоносные программы. [Электронный ресурс]. - Режим доступа: https://encyclopedia.kaspersky.ru/knowledge/malicious-programs (дата обращения - 22.07.2023).

Проиллюстрируем это на примере. В мае 2017 г. была осуществлена одна из наиболее масштабных за обозримое время атака с применением программы-шифровальщика WannaCry. Только за один день вредоносная программа атаковала компьютеры пользователей более чем в 74 странах. По своему основному предназначению WannaCry имеет те же функциональные возможности, что и другие шифровальщики, – модификация пользовательских данных на компьютере и последующее требование выкупа за их восстановление, но столь массовые случаи заражения были связаны со способом распространения.

Первичное заражение осуществлялось посредством эксплуатации уязвимости ОС Windows. После успешного проникновения хотя бы на один компьютер, подключенный к локальной сети, шифровальщик WannaCry распространялся по сети на другие устройства как червь (Worm). По этой причине наибольший ущерб от шифровальщика WannaCry был причинен организациям, имеющим крупные корпоративные компьютерные сети[29].

Программы, относящиеся к третьему подклассу, – троянские программы (Trojan programs) не умеют создавать свои копии и не способны к самовоспроизведению. В этом случае распространение копий по сети и заражение удаленных компьютеров происходит по команде с сервера управления.

Основным признаком, который служит для дифференцирования троянских программ, является вид действия (поведение), которое они выполняют на компьютере, например:

– программы-шпионы (Trojan-Spy) предназначаются для ведения электронного шпионажа за пользователем, в том числе перехвата вводимых с клавиатуры данных, изображений экрана, списка активных приложений;

[29] Чекунов И. Г., Рядовский И. А. и др. Методические рекомендации по расследованию преступлений в сфере компьютерной информации: учеб. пособие, 2-е изд. / под ред. И.Г. Чекунова. М.: Московский университет МВД России имени В.Я. Кикотя, 2019. С. 85-86.

– программы-банкеры (Trojan-Banker) создаются с целью поиска и копирования пользовательской информации, относящейся к банковским счетам, системам электронных денег и пластиковым картам;

– программы-шифровальщики (Trojan-Ransom) модифицируют пользовательские данные на компьютере либо блокируют работу компьютера с целью получения выкупа за восстановления доступа к информации;

– программы для удаленного управления (Trojan-Backdoor) обеспечивают скрытое удаленное управление компьютером и полный доступ к пользовательской информации;

– программы-загрузчики (Trojan-Downloader, Trojan-Dropper) осуществляют загрузку и установку на компьютер вредоносных программ и их новых версий;

– программы для эксплуатации программных уязвимостей (Exploit) эксплуатируют уязвимости программного обеспечения пользователя.

Большинство современных троянских программ сочетают в себе не одно поведение, а целый набор видов деятельности, предоставляющий преступникам самые широкие возможности для манипулирования пользовательской информацией. Например, программа-банкер, определяемая антивирусным программным обеспечением Лаборатории Касперского с именем Trojan-Banker.Win32.RTM, помимо присущей только этому виду троянских программ функциональности поиска и копирования пользовательской информации, относящейся к банковским счетам, системам электронных денег и пластиковым картам, обладает и многими другими возможностями – поиска файлов по именам, записи истории нажатий клавиш клавиатуры, записи видео и создании снимков экрана, копирования буфера обмена, блокирования и нарушения работы операционной системы, получения от сервера управления команд на запуск дополнительных программных модулей, отправки собранной информации на сервер управления и т.п.

Для загрузки троянских программ в компьютерную систему без ведома пользователя применяют различные способы.

Способы проникновения в систему:

– рассылка электронных писем, содержащих вредоносное вложение;

– применение связок эксплойтов при веб-серфинге пользователей в сети Интернет;

– внедрение вредоносного кода в распространяемое легальное программное обеспечение;

– распространение в локальной сети посредством применения штатных программных средств;

– физический доступ к целевой системе.

Для проникновения в систему с помощью сообщений электронной почты преступники осуществляют целевую либо массированную рассылку писем, содержащих в качестве вложения специальным образом, сформированный документ. Открытие пользователем данного документа приводит к скрытой загрузке вредоносной программы и установке ее в систему.

В другом варианте вредоносное письмо содержит не вложение, а ссылку на внешний Интернет-ресурс, при переходе по которой компьютер пользователя подвергается атаке набором эксплойтов (exploits). При успешном срабатывании одного из эксплойтов на компьютер пользователя загружается вредоносное программное обеспечение. При необходимости, когда возможности совершения несанкционированных действий на компьютере пользователя ограничены правами его учетной записи, преступниками может быть применен локальный эксплойт для повышения привилегий.

Для заражения компьютеров может быть использован так называемый метод drive-by загрузки, когда в процессе перемещения пользователя по сайтам в сети Интернет его компьютер скрыто перенаправляется с

легитимной, но скомпрометированной страницы на криминальный ресурс, где подвергается атаке набором эксплойтов.

Описанные способы наиболее распространены и хорошо известны. В более редких случаях преступники предварительно получают несанкционированный доступ к сетевым ресурсам разработчика легальных программ, после чего внедряют в распространяемое им программное обеспечение свой вредоносный код.

При наличии у преступников доступа хотя бы к одному компьютерному устройству локальной сети организации дальнейшее распространение вредоносных программ на другие компьютеры и серверы может осуществляться с помощью штатных программных средств и протоколов. Например, неоднократно фиксировалось использование программы PsExec от корпорации Microsoft для автоматизированного развертывания вредоносного программного обеспечения на всех компьютерах, входящих в корпоративную сеть.

Физический доступ к компьютерной системе может быть обеспечен вовлечением в преступление работника потерпевшей организации либо проникновением преступников за охраняемый периметр. В этом случае загрузка вредоносной программы в систему осуществляется посредством подключения к ней внешнего электронного носителя информации.

Помимо программных средств, в более редких случаях, способами компьютерных преступлений служат специально созданные в преступных целях электронно-вычислительные устройства и программы к ним. Подобные комплексы могут быть как достаточно простыми, например, устройства, скрыто устанавливающееся в разрыв интерфейса клавиатуры для перехвата нажатия клавиш, так и более сложными. Например, компьютерное устройство размером с USB-флеш-накопитель с собственным сетевым адаптером и установленной специальной программой удаленного управления предоставляет преступнику возможность получить несанкционированный доступ к удаленной компьютерной системе. Для этого устройство скрыто

подключается к целевой системе, например, корпоративной компьютерной сети в месте, исключающем его визуальное обнаружение, для чего нередко в преступление вовлекают работника пострадавшей организации.

К более сложным техническим решениям, создаваемым для совершения преступлений, применимо иное название – аппаратно-программные комплексы. К ним относятся так называемые бот-фермы, то есть компьютерные системы, эмулирующие работу большого количества устройств с отдельными каналами подключения к сети Интернет. Такие системы используются для массовых кампаний распространения вредоносного программного обеспечения на мобильные устройства под управлением ОС Android посредством СМС-рассылки либо для осуществления DDoS-атак.

Весьма существенную угрозу для банковской сферы на определенном этапе представляли аппаратно-программные комплексы, разработанные для совершения хищений денежных средств из банкоматов, – так называемые Black Box'ы. Такой комплекс является, по сути, миникомпьютером с установленным на него специальным программным обеспечением, который подключают к диспенсеру (механизму выдачи денег) вместо штатного компьютера, расположенного в сервисной зоне банкомата. После этого управление банкоматом может осуществляться с помощью технологий беспроводной передачи данных, например, со смартфона.

Глобальная сеть Интернет является всемирной системой объединенных компьютерных сетей, поэтому представляется необходимым уделить внимание таким способам осуществления несанкционированного доступа как компьютерные атаки на локальные сети.

Согласно Национальному стандарту ГОСТ Р 51275–2006 «Защита информации. Объект информатизации. Факторы, воздействующие на

информацию. Общие положения»[30] п.3.11 «под компьютерной атакой понимается целенаправленное несанкционированное воздействие на информацию, на ресурс автоматизированной информационной системы или получение несанкционированного доступа к ним с применением программных или программно-аппаратных средств». Фактически под признаки компьютерной атаки подпадают все способы осуществления несанкционированного доступа к компьютерным системам, упомянутые в настоящей статье. Однако именно атаки на локальные сети позволяют наиболее полно рассмотреть приемы и методы, используемые преступниками с этой целью.

Виды компьютерных атак на локальные корпоративные сети могут быть разными:

– внешняя атака на сетевую инфраструктуру организации либо на компьютерные системы, которым разрешено удаленное подключение к локальной сети;

– атака изнутри пострадавшей организации с участием ее работников;

– комбинированная атака, сочетающая в себе элементы обоих указанных выше способов совершения преступления.

Необходимо учитывать, что преступник, действующий внутри организации, может также использовать вредоносные программы, как и преступник внешний. С одной стороны, это усиливает его возможности, с другой – может ввести в заблуждение следствие относительно участия в преступлении инсайдера, если такие программы будут обнаружены в ходе осмотра места происшествия и при проведении судебной экспертизы. Участие инсайдера в преступлении не обязательно должно быть непосредственным. Работник организации может предоставить соучастникам

[30] ГОСТ Р 51275-2006. Национальный стандарт Российской Федерации. «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» (утв. и введен в действие Приказом Ростехрегулирования от 27.12.2006 № 374-ст.

необходимые сведения для осуществления несанкционированного доступа внутрь корпоративной компьютерной сети или сообщить об уязвимостях программного обеспечения, установленного на компьютерах организации, либо ошибках в настройках сетевого оборудования.

Функциональные возможности вредоносных программ и легальных условно-опасных программ, предоставляющих удаленный доступ к системе, позволяют проводить атаки на компьютерные системы без какого-либо вовлечения в этот процесс потерпевших. В этом случае реализация преступного умысла осуществляется втайне от них, а зачастую скрыта и от третьих лиц, так как происходит только на уровне машинной обработки и передачи компьютерной информации.

На этой основе способы киберпреступлений в зависимости от доступа к компьютерным средствам и системам следует делить на:

– способы, связанные с удаленным доступом к компьютерным средствам и системам посредством использования компьютерной коммуникационной сети (локальной или глобальной - Интернет);

– способы, связанные с непосредственным доступом к компьютерным средствам и системам.

В других случаях вовлечение потерпевшего, в той или иной степени, является необходимым условием доведения преступных намерений до конца. Непосредственная эксплуатация уязвимостей человеческого фактора предусматривает прямое общение с потерпевшим с применением навыков социальной инженерии, то есть системы психологических приемов и методов, склоняющих потерпевших к совершению определенных действий в интересах преступников, например, к разглашению уникального кода, присланного в Смс-сообщении для авторизации на сетевом ресурсе, либо к самостоятельной загрузке программы удаленного администрирования на свой компьютер и предоставлению реквизитов доступа к нему мошеннику.

Однако низкий уровень культуры информационной безопасности позволяет преступникам получать необходимые сведения для проведения

атаки и без прямого общения с потерпевшим. Использование ненадежных паролей, заводских настроек и конфигураций программного обеспечения и оборудования предоставляет широкий спектр возможностей для получения несанкционированного доступа к конфиденциальной информации. Так, один из широко известных и применяемых способов получения несанкционированного доступа к компьютерной сети – это проведение атаки с применением различных методов сканирования портов сетевых узлов, то есть виртуальных точек входа-выхода сетевого трафика, обслуживающих определенные локальные сервисы. Обнаружив в результате сканирования открытый порт, который обычно используется одной из распространенных программ удаленного администрирования, преступники могут получить доступ к системе перебором реквизитов доступа (пары: логин – пароль).

Для доступа к корпоративным компьютерным системам преступники могут воспользоваться и уязвимостью в организации охранных систем и регламентов предприятия, что может выражаться как в физическом проникновении за охраняемый периметр, так и в удаленном доступе с использованием разрешенных в организации к применению протоколов и программных средств. В связи с этим можно разграничить способы получения несанкционированного доступа к компьютерным системам и сетям по степени вовлеченности протерпевшего в этот процесс:

– эксплуатация уязвимостей аппаратного и программного обеспечения;

– использование недостатков организационного и технического характера корпоративных охранных систем;

– применение методов социальной инженерии.

Способы совершения «традиционных» преступлений с использованием информационно-коммуникационных технологий

Вместе с тем нельзя обойти вниманием все более возрастающую тенденцию в применении компьютерных и сетевых технологий как средств совершения преступлений, объектом которых выступают любые

общественные отношения, а не только отношения в сфере компьютерной информации. Данный факт находит свое отражение и в том, что эксперты в области информационной безопасности все чаще привлекаются в качестве специалистов при проведении следственных действий и оперативно-разыскных мероприятий по преступлениям традиционной направленности: убийствам, мошенничеству, незаконным организации и проведению азартных игр и т. п.[31]

Такая картина видится закономерной вследствие продолжающегося развития информационно-коммуникационных технологий, в том числе средств криптографии, что безусловно влияет на совершенствование средств защиты информации. Способы совершения компьютерных преступлений, которые успешно применялись еще 2–3 года назад, становятся неэффективными. Отходят на второй план и используются только в качестве вспомогательных распространенные еще в недавнем прошлом такие способы преступлений, как, например, перехват сетевого трафика, потерявший свою эффективность с точки зрения преступников в результате массового перехода сетевых сервисов с HTTP-протокола, предусматривающего открытую передачу данных, на протокол HTTPS, обеспечивающий шифрование сетевого трафика между конечными устройствами[32], либо браузерные атаки, ставшие нецелесообразными и сложными в исполнении в связи с предпринятыми разработчиками мерами, направленными на значительное повышение безопасности клиентского ПО.

В то же время появились новые возможности. Так, востребованными при совершении компьютерных преступлений становятся сервисы, построенные на базе облачных технологий. Облачные серверы позволяют сделать реализацию преступных планов более стабильной. Например, в случае блокировки учетной записи из-за многочисленных жалоб

[31] Семикаленова А.И., Рядовский И.А. Использование специальных знаний при обнаружении и фиксации цифровых следов: анализ современной практики // Актуальные проблемы российского права. 2019 (6). С. 178-185.

[32] Helme S. Alexa Top 1 Million Analysis - February 2018. [Электронный ресурс]. - Режим доступа: https://scotthelme.co.uk/alexa-top-1-million-analysis-february-2018 (дата обращения - 06.06.2023).

преступники быстро и без проблем могут перенести данные на другой сервер и продолжить свою преступную деятельность. При этом для настройки и поддержки сетевой инфраструктуры, используемой в противоправной деятельности, преступникам больше не нужен соучастник, выполняющий роль администратора компьютерной сети, его работу стал выполнять не осведомленный об их преступных намерениях поставщик услуг[33].

На фоне развития и внедрения информационно-коммуникационных технологий получили развитие различные способы совершения мошенничества.

Рассмотрим частный случай мошеннических действий, получивший свое собственное, хотя и неформальное название – телефонное мошенничество.

В общих словах телефонное мошенничество заключается в том, что обман потерпевшего осуществляется преступниками дистанционно – с помощью телефонной связи. Однако простое использование стационарных или мобильных телефонов не всегда может обеспечить конспиративность преступной деятельности, а также применение методов социальной инженерии, например когда для обмана потерпевшего требуется сокрытие телефонного номера, звонящего либо его подмена при определении входящего звонка. Для реализации таких замыслов преступники используют возможности IP-телефонии (технология VoIP – Voice over Internet Protocol). Сама по себе IP- телефония как технология (сетевые протоколы, ПО) является достаточно простой, однако ее использование совместно с иными технологиями, например VPN, предоставляет мошенникам широчайшие возможности для сокрытия следов преступной деятельности и применения методов психологического воздействия на потерпевших. Манипулируя

[33] Сабитов Р.Р. Развитие русскоязычной киберпреступности: что изменилось с 2016 по 2021 год. https://securelist.ru/russian-speaking-cybercrime-evolution-2016-2021/103920/ (дата обращения - 06.06.2023).

различными технологическими инструментами, преступники моделируют разнообразные схемы телефонной коммуникации[34].

В основе всех схем находится непосредственно протокол VoIP, реализация которого схожа с функционированием электронной почты. Однако, осознавая, что применение простой схемы приведет к их скорому разоблачению, мошенники обычно дополняют ее следующими элементами:

– прокси-серверы и VPN-серверы, шифрующие голосовой трафик и скрывающие адреса оконечных устройств;

– пограничное оборудование, позволяющее организовывать телефонные соединения между абонентами общетелефонной сети и IP-телефонии;

– виртуальные АТС, разделяющие сегменты многоэлементной сети IP-телефонии.

Виртуальная АТС, настраиваемая в большинстве случаев на базе свободно распространяемого ПО Asteriks, позволяет не только скрыть адреса оконечных устройств, но и осуществлять подмену номера при исходящем звонке. При этом регламенты проверки номеров провайдерами в некоторых иностранных государствах позволяют использовать любые номера без подтверждения. Так, в случае указания в данном поле номера телефона общеизвестного доверенного учреждения, исходящий вызов, транслированный в общетелефонную сеть через пограничное оборудование на территории иностранного государства, поступив на телефон российского пользователя, отобразится в подмененном виде, то есть вызов будет воспринят абонентом, как поступивший от доверенного лица.

Исследуя способы совершения компьютерных преступлений, было бы неправильным не обратить пристальное внимание на бурный рост суицидального контента, распространяющегося в социальных сетях в так называемых «группах смерти», представляющий особую общественную

[34] Чекунов И. Г., Рядовский И. А. и др. Методические рекомендации по расследованию преступлений в сфере компьютерной информации: учеб. пособие, 2-е изд. / под ред. И.Г. Чекунова. М.: Московский университет МВД России имени В.Я. Кикотя, 2019.

опасность, так как жертвами склонения к совершению самоубийства в сети Интернет в большинстве случаев становятся несовершеннолетние. По официальным данным, начиная с 2017 года, Роскомнадзором были заблокированы более чем 31 000 «групп смерти» и личных страниц пользователей, на которых были обнаружены информационные материалы с призывами к осуществлению самоубийства[35].

Следует отметить, что, начиная преимущественно с 2017 года, в социальных сетях «Вконтакте» и других начали появляться картинки с изображением китов с хештегами «Синий кит», «Разбуди меня в 4:20», «Я в игре», «Тихий дом», «Беги или умри», «Фея огня» и другими. Осуществляя переход по указанным ссылкам (хештегам), пользователи, как правило, несовершеннолетние переадресовывались на страницу или виртуальное сообщество, пропагандирующее склонение к совершению самоубийства, где в последующем подвергались вовлечению и вербовке со стороны кураторов этих групп, подталкивающих их к совершению суицида[36]. Отметим также, что пропаганда склонения к совершению самоубийства среди подростков сегодня все чаще осуществляется посредством использования теневого сегмента сети Интернет, так называемого «Даркнета», позволяющего посредством информационно-коммуникационных технологий анонимизировать свою сетевую активность.

С момента достижения поставленной цели кураторами «групп смерти» — совершения суицида несовершеннолетним, в более чем 90 % случав начинается «зачистка» следов преступления, заключающаяся в удалении: переписок (аудио-/видеосообщений), хранящихся на удаленных серверах; персональных страниц, с которых велась переписка куратора и потерпевшего; групп/сообществ, на которые была подписана жертва и т. д.

---

[35] Официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций [Электронный ресурс]. - Режим доступа: https://rkn.gov.ru/press/publications/news67418.htm (дата обращения: 06.06.2023).

[36] Пантюхина Г. А. К проблеме расследования уголовных дел, связанных с суицидальными действиями несовершеннолетних с использованием социальных сетей // ИСОМ. 2017. №2 - [Электронный ресурс]. - Режим доступа: https://cyberleninka.ru/ (дата обращения: 06.06.2023).

Доступ к персональной странице потерпевшего (логин и пароль), куратор получает от потерпевшего после его вовлечения в «игру» под видом прохождения одного из заданий. В дальнейшем эти данные используются для уничтожения информации, которая может привести следствие к конкретному лицу или сообществу/группе в социальной сети.

Таким образом, как видно из приведенных примеров, при совершении компьютерных преступлений различной направленности преступниками используются технологии, позволяющие анонимизировать свою противоправную активность в сети Интернет и предпринять действенные меры к сокрытию следов преступления.

Полагаем, что представленный анализ способов компьютерных преступлений наглядно показывает их полноструктурный характер. Основной криминалистической закономерностью формирования и реализации способа преступления с использованием информационных компьютерных технологий является то обстоятельство, что подготовка обычно предусматривает действия по сокрытию. То есть при совершении компьютерных преступлений, неважно относятся ли они к киберзависимым либо не относятся к таковыми, характерным является осуществление преступниками комплекса мер, предшествующих покушению на преступление, которые направлены на сокрытие его следов.

Применительно к способам компьютерных преступлений можно обозначить следующие закономерности:

– закономерности формирования и реализации способа преступления, совершаемого с использованием информационных компьютерных технологий (связь способа с личностью преступника, зависимость способа от конкретных обстоятельств совершения преступления и т. д.);

– закономерности отражения в компьютерных средствах и системах информации о связях действий и их результатов, повторяемости

действий в похожих ситуациях, стереотипов действий субъектов при совершении преступлений;

– закономерности возникновения и развития обстоятельств, связанных с преступлением, сопряженным с использованием компьютерных средств и систем (как до, так и после его совершения) и значимых для расследования.

4. Обзор судебной практики по уголовным делам о киберпреступлениях

1. Механическое воспрепятствование работе банкомата, выполняющего функции компьютера, является незаконным воздействием на него. Тем самым и по данному основанию такие действия не могли быть квалифицированы как кража с банковского счета, они подлежат переквалификации на ч. 1 ст. 159[3] УК РФ. Выводы суда о совершении 17 преступлений необоснованны, в связи с чем из приговора подлежит исключению назначение наказания по совокупности преступлений по правилам ч. 3 ст. 69 УК РФ[37].

Приговором Ленинского районного суда г. Тамбова от 19 мая 2021 года Г. осужден за каждое из 17 преступлений, предусмотренных п. «г» ч. 3 ст. 158 УК РФ, к 2 годам 6 месяцам лишения свободы; на основании ч. 3 ст. 69 УК РФ окончательно назначено 4 года лишения свободы в исправительной колонии строгого режима.

Апелляционным определением Тамбовского областного суда от 12 августа 2021 года приговор оставлен без изменения.

В кассационной жалобе осужденный Г. выражает несогласие с принятыми судебными решениями в части квалификации содеянного. Считает, что его действия должны быть квалифицированы по ч. 1 ст. 158 УК РФ. Помимо этого указывает, что все 17 хищений были им совершены одним

[37] Кассационное определение Второго кассационного суда общей юрисдикции от 01.04.2022 № 77-991/2022 // СПС «КонсультантПлюс» (дата обращения: 16.07.2023).

и тем же способом за непродолжительное время, а потому должны быть квалифицированы как одно преступление. Выражает несогласие и с назначенным наказанием. Просит внести в приговор соответствующие изменения и снизить ему наказание.

Судебная коллегия по уголовным делам Второго кассационного суда общей юрисдикции 1 апреля 2022 г. изменила приговор и апелляционное определение в отношении Г. по следующим основаниям.

В соответствии с разъяснениями, данными Верховным Судом Российской Федерации в п. 21 постановления Пленума от 30 ноября 2017 года № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» действия виновного подлежат квалификации как кража, если виновным не было оказано незаконного воздействия на программное обеспечение серверов, компьютеров или на сами информационно-телекоммуникационные сети. Суд, сославшись в приговоре на данные разъяснения, не принял во внимание, что механическое воспрепятствование Г. работе банкомата, выполняющего функции компьютера, является незаконным воздействием на него. Тем самым и по данному основанию действия Г. не могли быть квалифицированы как кража с банковского счета.

Как следует из показаний представителя потерпевшего Д. в банке существовала подача претензий на сумму до № рублей в автоматическом режиме, то есть без участия сотрудников банка по упрощенной системе урегулирования.

Внося заведомо ложные сведения о техническом сбое операционной системы банкомата в претензию, направленную через удаленные каналы обслуживания банка, Г. по сути обманывал банк. Согласно разъяснениям Верховного Суда РФ, содержащимся в п. 2 вышеназванного постановления Пленума, обман при мошенничестве может состоять в сознательном сообщении заведомо ложных, не соответствующих действительности сведений, либо в умышленных действиях, направленных на введение владельца имущества или иного лица в заблуждение. При этом диспозиция

ни ч. 1 ст. 159 УК РФ, ни ч. 1 ст. 159^3 УК РФ не содержит обязательного условия обмана непосредственно конкретного физического лица.

Помимо этого, судебная коллегия констатирует, что при одномоментном хищении таким способом чужого имущества на сумму свыше № рублей виновный должен был непосредственно явиться в офис банка и сообщить заведомо ложные сведения о техническом сбое в работе операционной системы банкомата одному из сотрудников. В этом случае его действия должны быть квалифицированы как мошенничество. Тем самым квалификация содеянного, как кража или мошенничество, зависела бы от размера похищенного, что противоречило бы уголовно-правовому принципу назначения более строгого наказания за более тяжкое преступление.

При таких обстоятельствах судебная коллегия не нашла оснований и для переквалификации действий Г. на ч. 1 ст. 158 УК РФ. Таким образом, действия Г. подлежат переквалификации на ч. 1 ст. 159^3 УК РФ, поскольку при хищении он использовал электронные средства платежа, которые впоследствии обналичивал.

Не основаны на исследованных в судебном заседании доказательствах и выводы суда о совершении Г. 17 преступлений. Действия Г. были тождественны, хищения совершались у одного потерпевшего, одним и тем же способом, совершены в короткий промежуток времени и были объединены единым умыслом.

Судебная коллегия определила: действия осужденного переквалифицировать на одно преступление по ч. 1 ст. 159^3 УК РФ, назначить наказание в виде 1 года 10 месяцев лишения свободы, исключить указание о применении положений ч. 3 ст. 69 УК РФ, вид рецидива изменить с опасного на простой, вводную часть дополнить указанием на судимость по предыдущему приговору.

2. Оплата чужой картой своих покупок не может трактоваться как мошенничество, так как у сотрудников торговых точек нет

обязанности идентификации держателя карты по документам, удостоверяющим его личность[38].

По приговору Индустриального районного суда г. Перми от 30 июля 2020 года Е. была осуждена по ч. 1 ст. 159^3 УК РФ к 1 году 6 месяцам лишения свободы; по п. «г» ч. 3 ст. 158 УК РФ к 3 годам лишения свободы; по п. «г» ч. 3 ст. 158 УК РФ к 2 годам 6 месяцам лишения свободы; по п. «а» ч. 3 ст. 158 УК РФ за совершение восьми преступлений к 2 годам 6 месяцам лишения свободы за каждое. В соответствии с ч. 3 ст. 69 УК РФ по совокупности преступлений путем частичного сложения наказаний окончательно Е. назначено 5 лет лишения свободы в исправительной колонии общего режима.

Апелляционным определением судебной коллегии по уголовным делам Пермского краевого суда от 29 сентября 2020 года приговор в отношении Е. изменен. Из осуждения исключен п. «а» ч. 3 ст. 158 УК РФ. На основании ч. 3 ст. 69 УК РФ по совокупности преступлений, предусмотренных ч. 1 ст. 159^3 УК РФ, п. «г» ч. 3 ст. 158 УК РФ (два преступления), п. «а» ч. 3 ст. 158 УК РФ (восемь преступлений), путем частичного сложения наказаний, окончательно Е. назначено 4 года 10 месяцев лишения свободы с отбыванием в исправительной колонии общего режима.

В кассационной жалобе осужденная Е. просит о пересмотре состоявшихся судебных решений, указывая, что суд необоснованно квалифицировал её действия, связанные с хищением денег с банковской карты потерпевшей С., дополнительно по ч. 1 ст. 159^3 УК РФ. Считает осуждение по данной статье излишним.

Кассационным определением судебной коллегии по уголовным делам Седьмого кассационного суда общей юрисдикции от 10 июня 2021 года приговор и апелляционное определение в отношении Е. оставлены без изменения.

[38] Кассационное определение Верховного Суда Российской Федерации от 04.08.2022 по делу № 44-УД22-21-К7 // СПС «КонсультантПлюс» (дата обращения: 21.07.2023).

Изучив материалы уголовного дела, обсудив доводы кассационной жалобы, Судебная коллегия по уголовным делам Верховного Суда РФ находит ее подлежащей удовлетворению по следующим основаниям.

23 января 2019 года Е. похитила банковскую карту потерпевшей и использовала ее для оплаты покупок в различных магазинах в период с 24 по 25 января 2019 года, на сумму 3 878 рублей. Указанные действия осужденной судом квалифицированы по ч. 1 ст. 159^3 УК РФ. Вместе с тем, по смыслу закона, хищение денежных средств, совершенное с использованием виновным электронного средства платежа, образует состав преступления, предусмотренного ст. 159^3 УК РФ, в тех случаях, когда изъятие денежных средств было осуществлено путем обмана или злоупотребления доверием их владельца или иного лица.

Между тем, из установленных судом обстоятельств, следует, что осужденная похитила банковскую карту, которой расплачивалась в торговых организациях. При этом работники магазинов участия в осуществлении операций по списанию денежных средств с банковского счета в результате оплаты товаров, не принимали и личность осужденной в качестве законного владельца карты не удостоверяли. Действующими нормативными актами на уполномоченных работников торговых организаций, осуществляющих платежные операции с банковскими картами, обязанность идентификации держателя карты по документам, удостоверяющим его личность, не возлагается.

В связи с этим Е. ложные сведения о принадлежности карты именно ей не сообщала сотрудникам торговых организаций и не вводила их в заблуждение, умолчав о том, что используемая ею карта принадлежит иному лицу.

С учетом изложенного, действия Е. по хищению всех денежных средств потерпевшей подлежали квалификации по п. «г» ч. 3 ст. 158 УК РФ и не требовали дополнительной квалификации по ч.1 ст. 159^3 УК РФ.

Судебная коллегия определила: исключить осуждение Е. по ч.1 ст. 159^3 УК РФ. Квалифицировать действия Е. по фактам хищения денежных средств, принадлежащих потерпевшей по п. «г» ч. 3 ст. 158 УК РФ, по которой назначить наказание в виде 3 лет лишения свободы. Окончательно назначить Е. 4 года 9 месяцев лишения свободы с отбыванием в исправительной колонии общего режима.

3. Криптовалюта признана предметом хищения[39].

По приговору Петроградского районного суда г. Санкт-Петербурга от 20 декабря 2021 года П. осужден за совершение преступления, предусмотренного п. «б» ч. 3 ст. 161 УК РФ, к наказанию в виде лишения свободы на срок 9 лет с отбыванием в исправительной колонии строгого режима.

Апелляционным определением судебной коллегии по уголовным делам Санкт-Петербургского городского суда от 16 мая 2022 года приговор оставлен без изменения.

В кассационной жалобе осужденный П. выражает несогласие с приговором и апелляционным определением ввиду неправильного применения уголовного закона при квалификации его действий и при назначении наказания. Осужденный отмечает, что фактическую сторону содеянного он в целом не отрицал, был не согласен лишь с юридической оценкой его действий как хищения имущества. В обоснование указывает, что криптовалюта не может быть признана «иным имуществом», как посчитал суд первой инстанции, в частности не может быть отнесены к категории «цифровых прав», поскольку преступление было совершено 03 июня 2018 года, а цифровые права были отнесены к имущественным правам положениями ст. 128 ГК РФ в редакции Федерального закона от 18 марта 2019 года № 34-ФЗ, после совершения преступления. Следовательно, оспариваемый вывод суда основан на признании обратной силы

[39] Кассационное определение Третьего кассационного суда общей юрисдикции от 06.06.2023 по делу № 77-1296/2023 // СПС «КонсультантПлюс» (дата обращения: 26.07.2023).

гражданского законодательства, что не допускается законом (ст. 4 ГК РФ). Полагает недопустимым возложение на него ответственности за деяние, которое на момент совершения преступлением не являлось.

Рассмотрев уголовное дело по кассационным жалобам осужденного П. и его защитников, судебная коллегия приходит к следующему.

Судебная коллегия не может согласиться с утверждениями авторов жалоб о необоснованности признания криптовалюты «иным имуществом», поскольку, несмотря на то, что криптовалюта как отдельный объект гражданского оборота в законе не поименована, однако общеизвестно, что она как актив представляет определенную имущественную ценность, возможен ее обмен на фиатные деньги или иные материальные блага в соответствии с правилами соответствующих онлайн-платформ.

Признание криптовалюты «иным имуществом» не противоречит ст. 128 ГК РФ, в том числе в редакции закона, действующего на момент совершения преступления, учитывая, что возможный перечень такого имущества не являлся и не является закрытым.

Отсутствие законодательного регулирования криптовалюты в виде «биткоинов», «дигибайтов», «битшейресов» и оценки их стоимости в законодательстве РФ, на что ссылается сторона защиты, не исключает квалификации действий по их противоправному безвозмездному изъятию и обращению в свою пользу как хищения, поскольку они имеют определенную имущественную ценность.

Таким образом, установив, что преступные действия осужденного были направлены на завладение криптовалютой, путем принуждения потерпевшего к переводу ее на электронные кошельки, суд правомерно квалифицировал содеянное именно как хищение чужого имущества, причинившее ущерб его владельцу.

Судебная коллегия определила: кассационную жалобу удовлетворить частично, смягчить назначенное П. наказание по п. «б» ч. 3 ст. 161 УК РФ до 8 лет 9 месяцев лишения свободы[40].

4. Вопреки доводам осужденного, суд не поддержал факт отсутствия доказательств, подтверждающих наличие квалифицирующих признаков преступления, предусмотренных ст. 171[2] УК РФ, как «совершенного с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет» и «группой лиц по предварительному сговору»[41].

12 апреля 2022 года приговором Автозаводского районного суда города Тольятти Самарской области Г. осуждена по ч. 2 ст. 171[2] УК РФ к 3 годам лишения свободы условно с испытательным сроком 2 года 6 месяцев, со штрафом в размере 100 000 рублей; Р. осуждена по ч. 2 ст. 171[2] УК РФ к 2 годам 6 месяцам лишения свободы условно с испытательным сроком 2 года.

18 августа 2022 года апелляционным постановлением Самарского областного суда приговор суда первой инстанции от 12 апреля 2022 года в отношении Р. и Л. изменен. Исключено из описательно-мотивировочной части приговора, при описании преступного деяния, признанного судом доказанным, указание о том, что Р. и Л. совершили незаконную организацию азартных игр. В остальной части приговор оставлен без изменения.

Приговором также осуждена Л. (С.), в отношении которой приговор и апелляционное постановление в кассационном порядке не обжалуются.

Г. признана виновной в незаконной организации и проведении азартных игр с использованием игрового оборудования вне игорной зоны, с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет», группой лиц по предварительному сговору.

---

[40] Несмотря на то, что среди рассматриваемого в настоящем исследовании перечня киберпреступлений грабеж не указан в качестве такового, представляется, что признав криптовалюту предметом грабежа, она может являться предметом преступного посягательства и в других формах хищения, например, при совершении кражи. Поэтому рассмотрение соответствующих судебных актов в п. 3 исследования имеет место и представляет важное значение для дальнейшей работы по расширению перечня киберпреступлений.

[41] Постановление Шестого кассационного суда общей юрисдикции от 12.01.2023 № 77-98/2023 // СПС «КонсультантПлюс» (дата обращения: 26.07.2023).

Р. с учетом апелляционного постановления признана виновной в незаконном проведении азартных игр с использованием игрового оборудования вне игорной зоны, с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет», группой лиц по предварительному сговору.

В кассационной жалобе осужденная Г. выражает несогласие с вышеуказанными судебными решениями, считая их незаконными, необоснованными и несправедливыми, постановленными с существенными нарушениями уголовного и уголовно-процессуального закона, повлиявшими на исход дела. Обращает внимание на отсутствие доказательств, подтверждающих наличие квалифицирующих признаков преступления, предусмотренных ст. 171^2 УК РФ, как «совершенного с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет» и «группой лиц по предварительному сговору».

В кассационной жалобе защитник-адвокат выражает несогласие с вышеуказанными судебными решениями и в отношении Р., считая их незаконными, необоснованными и несправедливыми, постановленными с существенными нарушениями уголовного и уголовно-процессуального закона, повлиявшими на исход дела. Ссылаясь на показания Р., указывает, что разницу между азартными играми и букмекерской деятельностью она не понимает, какого-либо опыта работы либо познаний в данных сферах не имеет. Считает, что все неустранимые сомнения в виновности его подзащитной должны толковаться в ее пользу.

Заслушав участников судебного разбирательства, проверив материалы уголовного дела, изучив доводы, изложенные в кассационных жалобах, суд кассационной инстанции приходит к следующим выводам.

Вывод суда о виновности Г. и Р. в совершении ими преступления, предусмотренного ч. 2 ст. 171^2 УК РФ, подтверждается совокупностью доказательств, представленных стороной обвинения.

Кроме того, виновность осужденных Г. и Р. в совершении ими преступления, предусмотренного ч. 2 ст. 171^2 УК РФ, подтверждается заключением эксперта, протоколами следственных действий и иными документами, исследованными в судебном заседании и указанными в приговоре, в том числе: рапортом об обнаружении признаков данного преступления; протоколом осмотра места происшествия; материалами оперативно-розыскных мероприятий (далее ОРМ), проведенных сотрудниками полиции, в том числе ОРМ «Проверочная закупка», протоколом осмотра предметов и документов, приобщенных к уголовному делу в качестве доказательств, заключением эксперта № от ДД.ММ.ГГГГ, из которого следует, что изъятое в ходе осмотра места происшествия и представленное эксперту оборудование является игровым оборудованием в соответствии с федеральным законом от 29 декабря 2006 года № 244-ФЗ. Информация о результате игр (торговли) генерируется на представленном оборудовании, а через сеть Интернет передаются и принимаются фискальные и технические данные. Совокупность программно-аппаратных средств является игровыми автоматами и не предназначено для проведения букмекерской деятельности. На представленном оборудовании установлены программы, предусматривающие возможность осуществлять организацию и проведение азартных игр, результат которых определяется в ходе розыгрыша устройством (программой), находящейся внутри оборудования.

Суд определил: приговор Автозаводского районного суда г. Тольятти Самарской области от 12 апреля 2022 года и апелляционное постановление Самарского областного суда от 18 августа 2022 года в отношении Г. и Р. оставить без изменения, кассационные жалобы осужденной Г. и защитника-адвоката, действующего в интересах осужденной Р. без удовлетворения.

5. Установив, что действия, связанные с публичными призывами к осуществлению террористической деятельности и оправданием терроризма в сети «Интернет», совершались виновным каждый раз с

вновь возникшим умыслом, суд правомерно квалифицировал их как самостоятельные преступления[42].

По приговору 2-го Западного окружного военного суда от 13 декабря 2021 г., оставленному без изменения апелляционным определением апелляционного военного суда от 16 марта 2022 г., Б. осужден за публичные призывы к осуществлению экстремистской деятельности, совершенные 10 ноября 2019 г. и 13, 20 апреля 2020 г., а также за публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма и его пропаганду, совершенные 27, 28 июня, 1 и 5 июля 2020 г. с использованием информационно-телекоммуникационной сети «Интернет» в г. Череповце Вологодской области, г. Сибае Республики Башкортостан и г. Костроме.

Судом действия Б. квалифицированы как два самостоятельных преступления, предусмотренные ч. 2 ст. 280 УК РФ, и три самостоятельных преступления, предусмотренные ч. 2 ст. 205^2 УК РФ.

В кассационной жалобе осужденный и его защитник просили приговор и апелляционное определение изменить, переквалифицировать содеянное Б. на два преступления, предусмотренные ч. 2 ст. 205^2 и ч. 2 ст. 280 УК РФ, и, соответственно, смягчить наказание.

Квалифицируя содеянное осужденным как пять самостоятельных преступлений, суд правомерно исходил из того, что он размещал в социальной сети материалы в разное время, в том числе через достаточно длительные промежутки между публикациями, при этом его действия имели различную направленность, мотивацию и характер с точки зрения признаков совершенных им преступлений.

Данный вывод суда подтверждается в том числе исследованными в суде показаниями Б. В частности, осужденный показал, что постоянно следил

[42] Обзор судебной практики Верховного Суда Российской Федерации № 1 (2023) (утв. Президиумом Верховного Суда РФ 26.04.2023), (Определение Судебной коллегии по делам военнослужащих № 222-УД22-47-А6) // СПС «КонсультантПлюс» (дата обращения: 26.07.2023).

за общественно-политической обстановкой в стране и получал информацию из различных источников в сети «Интернет», нервно и агрессивно воспринимает происходящие события. Написание им размещенных на своей странице стихотворений было обусловлено несколькими причинами. Например, стихотворение, размещенное 10 ноября 2019 г., написано в результате увлечения его в тот период религиозной мусульманской литературой и просмотром роликов, выпускаемых террористическими организациями. Кроме того, в зависимости от своего эмоционального состояния, а также под воздействием алкогольного опьянения он периодически удалял и восстанавливал свою страницу в социальной сети. В последний раз он удалил свою страницу непосредственно перед задержанием, так как ему надоело его «творчество».

Проанализировав показания осужденного в совокупности с другими исследованными в судебном заседании доказательствами, суд первой инстанции пришел к правильному выводу о том, что действия, за которые осужден Б., совершались им каждый раз с вновь возникшим умыслом.

При таких данных приведенные в кассационных жалобах доводы о необходимости квалификации содеянного осужденным как двух единых продолжаемых преступлений, предусмотренных ч. 2 ст. 280 и ч. 2 ст. 205^2 УК РФ, являются несостоятельными.

Судебная коллегия определила: приговор и апелляционное определение оставить без изменения.

6. Квалификация действий по производству наркотического средства по признаку с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет») является необоснованной и подлежит исключению из приговора[43].

[43] Определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 27.10.2022 № 24-УД22-12 // СПС «КонсультантПлюс» (дата обращения: 28.07.2023).

По приговору Верховного Суда Республики Адыгея от 6 апреля 2022 года Б. осужден по ч. 5 ст. 228^1 УК РФ к 15 годам лишения свободы, по ч. 2 ст. 228^3 УК РФ к обязательным работам сроком 180 часов.

На основании ч. 3 ст. 69 УК РФ по совокупности преступлений путем частичного сложения наказаний окончательно назначено 15 лет 10 суток лишения свободы в исправительной колонии строгого режима.

По приговору суда Б. осужден за производство наркотических средств, с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет»), организованной группой и в особо крупном размере, а также за незаконное хранение прекурсоров наркотических средств в особо крупном размере.

В апелляционном порядке приговор не обжаловался.

В кассационной жалобе осужденный Б. считает приговор незаконным и необоснованным вследствие чрезмерно суровым наказании.

Заслушав стороны, изучив доводы жалобы и возражений, проверив материалы дела, Судебная коллегия отмечает следующее.

Как правильно установил суд, Б. по указанию и под непосредственным руководством иных лиц, действуя в составе организованной группы, посредством сети «Интернет» для производства и сбыта наркотических средств приобрел соответствующее оборудование. Затем в этих же целях в своем домовладении приспособил обособленное помещение, в котором в период с марта по сентябрь 2020 г. незаконно производил для последующего сбыта соответствующее наркотическое средство.

Квалификация действия Б. как производство наркотического средства, организованной группой, в особо крупном размере и незаконное хранение прекурсоров наркотических средств в особо крупном размере является правильной и основана на установленных фактических обстоятельствах, в жалобе не оспаривается, как не оспаривается и вина.

Квалифицирующие признаки производства наркотического средства организованной группой, в особо крупном размере и незаконного хранения

прекурсоров наркотических средств в особо крупном размере мотивированы надлежащим образом.

В то же время квалификация действий Б. по производству наркотического средства по признаку с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет») является необоснованной.

Исходя из диспозиции статьи 228^1 УК РФ указанный квалифицирующий признак предусмотрен лишь применительно к сбыту наркотических средств, психотропных веществ или их аналогов.

В этой связи данный квалифицирующий признак подлежит исключению из осуждения Б. по ч. 5 ст. 228^1 УК РФ.

Судебная коллегия определила: исключить из осуждения по ч. 5 ст. 228^1 УК РФ квалифицирующий признак – с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет»). Смягчить назначенное по ч. 5 ст. 228^1 УК РФ наказание с применением ст. 64 УК РФ до 12 лет лишения свободы. На основании ч. 3 ст. 69 УК РФ по совокупности преступлений путем частичного сложения назначенных по ч. 5 ст. 228^1 УК РФ и ч. 2 ст. 228^3 УК РФ наказаний окончательно Б. назначить 12 лет 10 дней лишения свободы в исправительной колонии строгого режима.

7. Само по себе использование сети «Интернет» для достижения договоренности с кем-либо о приобретении наркотических средств, предназначенных для дальнейшего сбыта, равно как и для получения сведений о местонахождении указанных наркотических не свидетельствует о наличии указанного признака[44].

Приговором Кировского районного суда г. Казани Республики Татарстан от 3 июня 2020 года Г. осужден к лишению свободы по ч. 3 ст. 30, п. «г» ч. 4 ст. 228^1 УК РФ на восемь лет; по ч. 3 ст. 30, ч. 1 ст. 161 УК РФ на один год.

[44] Определение Шестого кассационного суда общей юрисдикции от 09.09.2021 № 77-3872/2021 // СПС «КонсультантПлюс» (дата обращения: 28.07.2023).

На основании ч. 2 ст. 69 УК РФ по совокупности преступлений, путем частичного сложения назначенных наказаний, назначено Г. наказание в виде лишения свободы сроком на восемь лет шесть месяцев.

В соответствии с приговором Г. признан виновным и осужден за незаконный оборот наркотических средств в виде сбыта в крупном размере с использованием информационно-телекоммуникационных сетей, группой лиц по предварительному сговору, а также в покушении на открытое хищение имущества из магазина.

Апелляционным определением судебной коллегии по уголовным делам Верховного Суда Республики Татарстан от 4 декабря 2020 года приговор в отношении Г. изменен: наказание Г. смягчено по ч. 3 ст. 30 п. «г» ч. 4 ст. 228^1 УК РФ до семи лет 11 месяцев лишения свободы, по ч. 3 ст. 30 ч. 1 ст. 161 УК РФ до одиннадцати месяцев лишения свободы; на основании ч. 2 ст. 69 УК РФ по совокупности преступлений назначено восемь лет четыре месяца лишения свободы; на основании ст. 70 УК РФ по совокупности приговоров к назначенному наказанию частично присоединено неотбытая часть наказания по приговору от 21 января 2019 года и окончательно назначено восемь лет десять месяцев лишения свободы.

В кассационной жалобе осужденный Г. выражает несогласие с состоявшимися в отношении него судебными решениями.

Проверив материалы уголовного дела, обсудив доводы кассационной жалобы, заслушав участников процесса, судебная коллегия приходит к следующему.

По смыслу уголовного закона квалифицирующий признак «с использованием электронных и информационно-телекоммуникационных сетей (включая сеть «Интернет»)» предполагает непосредственное выполнение лицом объективной стороны сбыта наркотических средств с использованием указанных сетей. При этом само по себе использование сети «Интернет» для достижения договоренности с кем-либо о приобретении наркотических средств, предназначенных для дальнейшего сбыта, равно как

и для получения сведений о местонахождении указанных наркотических не свидетельствует о наличии указанного признака.

Согласно положениям ч.ч. 3 и 4 ст. 14 УПК РФ все сомнения в виновности обвиняемого, которые не могут быть устранены в установленном уголовно-процессуальном законом порядке, должны толковаться в пользу обвиняемого. Приговор суда не может быть основан на предположениях.

В связи с чем из осуждения Г. подлежит исключению квалифицирующий признак «с использованием электронных и информационно-телекоммуникационных сетей (включая сеть «Интернет»)», а назначенное наказание смягчению.

Судебная коллегия определила: исключить из описания преступного деяния, признанного доказанным, и из квалификации содеянного по ч. 3 ст. 30, п. «г» ч. 4 ст. 228^1 УК РФ квалифицирующий признак «с использованием электронных и информационно-телекоммуникационных сетей (включая сеть «Интернет»)»; смягчить назначенное наказание Г. по ч. 3 ст. 30, п. «а» ч. 3 ст. 228^1 УК РФ до семи лет девяти месяцев лишения свободы; на основании ч. 2 ст. 69 УК РФ назначить Г. путем частичного сложения наказание в виде лишения свободы на срок восемь лет два месяца; на основании ст. 70 УК РФ по совокупности приговоров к назначенному наказанию частично присоединено неотбытая часть наказания по приговору от 21 января 2019 года и окончательно назначено восемь лет восемь месяцев лишения свободы.

8. Приобретение в свое пользование для сбыта произведенного наркотического средства Интернет-магазина свидетельствует о наличии умысла на ведение длительной деятельности, направленной не на разовое изготовление наркотического средства, а на систематическое, серийное его производство[45].

По приговору Московского областного суда от 21 июня 2022 г. Ш. осужден по ч. 5 ст. 228^1 УК РФ к 15 годам лишения свободы; по ч. 2 ст. 228^3

[45] Кассационное определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 11.07.2023 № 4-УД23-30-А1 // СПС «КонсультантПлюс» (дата обращения: 15.08.2023).

УК к 1 году ограничения свободы с возложением ограничений; по совокупности преступлений на основании ч. 3 ст. 69 УК РФ окончательно к 15 годам 3 месяцам лишения свободы с отбыванием наказания в исправительной колонии строгого режима.

Апелляционным определением судебной коллегии по уголовным делам Первого апелляционного суда общей юрисдикции от 21 сентября 2022 г. приговор в отношении Ш. оставлен без изменения, а апелляционные жалобы осужденного и его защитника – без удовлетворения.

По приговору Ш. признан виновным в незаконном производстве наркотических средств, совершенном группой лиц по предварительному сговору в особо крупном размере и в незаконном хранении прекурсоров наркотических средств в особо крупном размере при установленных в приговоре обстоятельствах.

В кассационной жалобе адвокат, выражая несогласие с постановленными в отношении его подзащитного приговором и апелляционным определением, настаивает на признании их вынесенными с нарушением требований уголовного закона и несправедливыми. Утверждает, что в действиях Ш. отсутствует состав незаконного производства наркотического средства, поскольку его действия не носили систематического, серийного характера. Полагает, что сам по себе факт покупки Ш. Интернет-магазина «<...>» не свидетельствует о наличии у него умысла на производство наркотических средств.

Изучив материалы уголовного дела и рассмотрев доводы, изложенные в кассационной жалобе защитника осужденного и в возражениях на нее, а также выслушав мнения сторон в судебном заседании, Судебная коллегия приходит к следующему.

Как установлено органами предварительного следствия и судом, Ш. совместно с неустановленными соучастниками в период не позднее 28 января 2021 г. оборудовал на чердаке гаража лабораторию с системой вентиляции, рассчитанную на длительный срок эксплуатации; приобрел

значительное число лабораторного оборудования, прекурсоров и иных химических препаратов, необходимых для производства наркотических средств, а также приобрел в свое пользование для сбыта произведенного наркотического средства Интернет-магазин «<...>» на сайте «<...>», что свидетельствует о наличии у Ш. умысла на ведение длительной деятельности, направленной не на разовое изготовление наркотического средства, а на систематическое, серийное его производство. Об этом же свидетельствует и содержание переписки Ш. с абонентами, с которыми он в течение периода с октября 2018 г. по 28 января 2021 г. обсуждал технологию производства наркотических средств и результаты собственной деятельности.

Оснований для признания назначенного осужденному наказания несправедливым и не соответствующим закону не усматривается.

Судебная коллегия определила: приговор Московского областного суда от 21 июня 2022 г. и апелляционное определение судебной коллегии по уголовным делам Первого апелляционного суда общей юрисдикции от 21 сентября 2022 г. в отношении Ш. оставить без изменения, а кассационную жалобу защитника осужденного – без удовлетворения.

9. При сбыте наркотических средств бесконтактным способом через тайники преступление считается оконченным с момента передачи приобретателю информации о месте его нахождения[46].

По приговору Кировского районного суда г. Астрахани от 11 октября 2018 года Д. осужден к лишению свободы по п. «а» ч. 4 ст. 228^1 УК РФ (по преступлению в период до 19 ч. 50 мин. 29.08.2017 г.) к 10 годам; п. «а» ч. 4 ст. 228^1 УК РФ (по преступлению в период до 19 ч. 40 мин. 18.09.2017 г.) к 10 годам; п. п. «а», «г» ч. 4 ст. 228^1 УК РФ к 10 годам 6 месяцам; ч. 3 ст. 30, п. п. «а», «г» ч. 4 ст. 228^1 УК РФ к 9 годам 6 месяцам; п. «а» ч. 3 ст. 174^1 УК РФ к 2 годам. На основании ч. 3 ст. 69 УК РФ по совокупности преступлений

[46] Определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 14.02.2023 № 25-УД22-36-К4 // СПС «КонсультантПлюс» (дата обращения: 15.08.2023).

путем частичного сложения наказаний назначено 12 лет 6 месяцев лишения свободы.

По делу также осуждена К., судебные решения в отношении которой не обжалованы.

Апелляционным определением судебной коллегии по уголовным делам Астраханского областного суда от 6 декабря 2018 года приговор в отношении Д. изменен. На основании ч. 3.2 ст. 72 УК РФ в редакции ФЗ от 3 июля 2018 г. № 186-ФЗ время содержания под стражей с 1 октября 2017 г. по день вступления приговора в силу 6 декабря 2018 г. зачтено в срок лишения свободы из расчета один день за один день. В остальном приговор оставлен без изменения.

Кассационным определением судебной коллегии по уголовным делам Четвертого кассационного суда общей юрисдикции от 12 июля 2021 года вышеуказанные судебные решения в отношении Д. изменены. Его действия по преступлению от 25.09.2017 г. переквалифицированы с п. п. «а», «г» ч. 4 ст. 228^1 УК РФ на ч. 3 ст. 30, п. п. «а», «г» ч. 4 ст. 228^1 УК РФ, по которой назначено наказание в виде лишения свободы сроком на 9 лет 9 месяцев. Назначенное на основании ч. 3 ст. 69 УК РФ по совокупности преступлений путем частичного сложения наказаний наказание смягчено до 11 лет 9 месяцев. Окончательное наказание, назначенное в соответствии с ч. 5 ст. 74, ст. 70 УК РФ, определено в виде лишения свободы сроком на 12 лет 3 месяца. В остальном приговор и апелляционное определение оставлены без изменения.

В кассационной жалобе осужденный Д., не оспаривая фактические обстоятельства, доказанность вины, не согласен с квалификацией своих действий по эпизоду от 18 сентября 2017 г. как оконченное преступление. Указывает, что информацию о месте расположения тайника с наркотиками соучастница К. сообщила только ему, Д., как участнику группы, а не приобретателю, в связи с чем, действия подлежат квалификации как покушение.

Проверив материалы дела, изучив доводы кассационной жалобы, заслушав стороны, Судебная коллегия находит судебные решения в отношении Д. подлежащими изменению по следующим основаниям.

Как установил суд, обнаруженные по месту проживания Д. и К. наркотические средства были ими ранее изъяты из тайника, перемещены домой, и предназначались для последующей реализации. В этой связи, поскольку Д. уже совершил ряд действий (изъял, т.е. приобрел, переместил к себе домой), составляющих объективную сторону сбыта, его действия правильно квалифицированы как покушение, а не приготовление, на сбыт наркотического средства.

Вместе с тем судебные решения в отношении Д. в части квалификации его действий по эпизоду от 18 сентября 2017 года подлежат изменению. Как установил суд, Д., являясь участником организованной группы, занимающейся незаконным сбытом наркотических средств через созданный интернет-магазин, имея умысел на незаконный сбыт наркотических средств, 18 сентября 2017 г. до 19 ч. 40 мин. извлек с соучастницей из тайника наркотическое средство массой 0.53 гр., которое в целях его незаконного сбыта соучастница с ведома и согласия Д. поместила в тайник в кустах у второго окна у <...> по <...>. В тот же день в период с 19 ч. 40 мин. до 20 ч. 15 мин. в ходе проведения осмотра места происшествия наркотическое средство было изъято сотрудниками УМВД по г. <...>.

Данные действия квалифицированы как оконченное преступление – по п. «а» ч. 4 ст. 228^1 УК РФ, то есть, незаконный сбыт наркотических средств, совершенный организованной группой, с использованием информационно-телекоммуникационных сети «Интернет», в значительном размере.

Однако по смыслу уголовного закона при сбыте наркотических средств бесконтактным способом через тайники преступление считается оконченным с момента передачи приобретателю информации о месте его нахождения.

Судом установлено, что непосредственно в тайник наркотическое средство было помещено К., которая сообщила об этом Д.. Тот, в свою

очередь, согласно распределенным ролям, должен был сообщить о месте нахождения тайника приобретателю. Однако преступная деятельность обоих была пресечена сотрудниками правоохранительных органов, и помещенное К. в тайник наркотическое средство было изъято. Доказательств о передаче Д. информации о месте нахождения тайника с наркотическим средством потенциальному приобретателю в приговоре не приведено, в связи с чем, действия Д. подлежат переквалификации.

Допущенная судом первой инстанции ошибка в части неправильной квалификации действий не была устранена судами апелляционной и кассационной инстанций, в связи с чем, судебные решения подлежат изменению, действия – переквалификации с назначением наказания, при котором Судебная коллегия учитывает установленные судом первой инстанции обстоятельства, а также положения ч. 1 ст. 62 и ч. 3 ст. 66 УК РФ.

Судебная коллегия определила: приговор Кировского районного суда г. Астрахани от 11 октября 2018 года, апелляционное определение судебной коллегии по уголовным делам Астраханского областного суда от 6 декабря 2018 года и кассационное определение судебной коллегии по уголовным делам Четвертого кассационного суда общей юрисдикции от 12 июля 2021 года в отношении Д. изменить.

Переквалифицировать действия Д. по преступлению от 18.09.2017 г. с п. «а» ч. 4 ст. 228^1 УК РФ на ч. 3 ст. 30, п. «а» ч. 4 ст. 228^1 УК РФ, по которой назначить наказание в виде лишения свободы на 9 лет.

На основании ч. 3 ст. 69 УК РФ по совокупности преступлений путем частичного сложения назначенных по п. «а» ч. 4 ст. 228^1 УК РФ (по преступлению от 29.08.2017 г.), по ч. 3 ст. 30, п. «а» ч. 4 ст. 228^1 УК РФ (по преступлению от 18.09.2017 г.), по ч. 3 ст. 30, п. п. «а», «г» ч. 4 ст. 228^1 УК РФ (по преступлению от 25.09.2017 г.), по ч. 3 ст. 30, п. «а», «г» ч. 4 ст. 228^1 УК РФ (в отношении наркотических средств, обнаруженных и изъятых 25.09.2017 г. по месту временного проживания в <...>), по п. «а» ч. 3 ст. 174^1 УК РФ наказаний назначить Д. 10 лет 6 месяцев лишения свободы.

10. Факт того, что осужденный никому не предлагал и не передавал видеофайл порнографического характера, а лишь разместил на него ссылку в открытом доступе на своей странице, не свидетельствует об отсутствии у него умысла на незаконный оборот порнографических материалов, поскольку он позволял другим пользователям сети «Интернет» просматривать содержание указанного видеофайла[47].

По приговору Октябрьского районного суда г. Архангельска от 27 июля 2021 года П. осужден по п. «б» ч. 3 ст. 242 УК РФ с применением ст. 73 УК РФ к 2 годам лишения свободы условно с испытательным сроком 2 года.

Апелляционным определением судебной коллегии по уголовным делам Архангельского областного суда от 13 октября 2021 года приговор оставлен без изменения.

Кассационным определением судебной коллегии по уголовным делам Третьего кассационного суда общей юрисдикции от 17 февраля 2022 года приговор от 27 июля 2021 года и апелляционное определение от 13 октября 2021 года в отношении П. отменены, уголовное дело в отношении П. по п. «б» ч. 3 ст. 242 УК РФ прекращено на основании п. 2 ч. 1 ст. 24 УПК РФ за отсутствием в деянии состава преступления, с признанием за ним в соответствии со ст. 133, 134 УПК РФ права на реабилитацию.

В кассационном представлении заместителя Генерального прокурора Российской Федерации Т. поставлен вопрос об отмене кассационного определения и направлении дела на новое кассационное рассмотрение в тот же суд в ином состава. В обоснование представления указывается, что вывод суда кассационной инстанции об отсутствии у П. прямого умысла на распространение порнографических материалов, поскольку загруженный П. видеофайл уже был распространен в сети «Интернет» и находился в свободном доступе, а сам П. никому его не предлагал и не передавал, является несостоятельным.

[47] Кассационное определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 08.12.2022 № 1-УДП22-10-К3 // СПС «КонсультантПлюс» (дата обращения: 31.07.2023).

Проверив материалы дела, обсудив доводы жалобы, Судебная коллегия приходит к следующему.

П., обладая знаниями в области информационных технологий и навыками пользователя компьютерной техники, являясь зарегистрированным пользователем социальной сети «<...>» под вымышленным именем «<...>», с целью незаконного распространения и публичной демонстрации порнографических материалов среди пользователей сети, разместил на своей странице для неограниченного круга пользователей в доступном для всеобщего обозрения и копирования разделе «Мои видеозаписи» ссылку на видеофайл, содержащий в соответствии с заключением экспертов информацию порнографического содержания. При этом П. не ограничил доступ других пользователей к своей странице со ссылкой на видеофайл порнографического содержания, который длительное время сохранялся в свободном доступе, создав возможность просмотра указанного видеофайла неограниченным количеством пользователей.

С данным выводом согласился и суд апелляционной инстанции.

Не оспаривая фактические обстоятельства дела, суд кассационной инстанции вышеуказанные судебные решения в отношении П. отменил и прекратил производство по уголовному делу, указав, что поскольку загруженный П. видеофайл уже был распространен в сети «Интернет» и находился в свободном доступе, сам П. никому его не предлагал и не передавал, то, следовательно, у П. отсутствовал умысел на незаконный оборот порнографических материалов.

Однако сделав такой вывод, суд кассационной инстанции не учел, что распространение материалов с порнографическим изображением, образующее объективную сторону преступления, предусмотренного ст. 242 УК РФ, может быть осуществлено посредством использования информационно-телекоммуникационной сети - технологической системы, предназначенной для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Распространение информации представляет собой как передачу информации неопределенному кругу лиц, так и действия, направленные на получение информации неопределенным кругом лиц.

Таким образом, судом кассационной инстанции оставлено без внимания, что П., будучи осведомленным об ответственном размещении любой информации, в том числе ссылок (репостов) на персональной странице и возможности наступления правовых последствий, проигнорировал Правила, разместил и длительное время хранил на ней в открытом доступе ссылку на видеофайл порнографического характера, оставив возможность доступа к своей странице любого пользователя сети «Интернет», при этом ограничения на доступ к своей странице им не устанавливались.

Судебная коллегия определила: представление заместителя Генерального прокурора Российской Федерации Т. удовлетворить, кассационное определение судебной коллегии по уголовным делам Третьего кассационного суда общей юрисдикции от 17 февраля 2022 года в отношении П. отменить, уголовное дело направить на новое судебное рассмотрение в суд кассационной инстанции иным составом суда со стадии судебного разбирательства.

11. Под распространением порнографических материалов в статье 242[1] УК РФ понимается, в том числе, незаконное предоставление возможности их использования неопределенному кругу лиц, которое может совершаться путем размещения на личных страницах и на страницах групп пользователей в социальных сетях ссылки для копирования файлов порнографического содержания[48].

По приговору Лискинского районного суда Воронежской области от 8 апреля 2021 г. (оставленному без изменения судом апелляционной

[48] Обзор судебной практики Верховного Суда Российской Федерации № 2 (2023) (утв. Президиумом Верховного Суда РФ 19.07.2023), (Кассационное определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 22.03.2022 № 14-УДП22-1-К1) // СПС «КонсультантПлюс» (дата обращения: 31.07.2023).

инстанции) Н., признан невиновным и оправдан по обвинению в совершении преступления, предусмотренного п. «г» ч. 2 ст. 242^1 УК РФ, на основании п. 2 ч. 1 ст. 24 УПК РФ в связи с отсутствием в его действиях состава преступления.

В соответствии со ст. 133, 134 УПК РФ за Н. признано право на реабилитацию.

Определением судебной коллегии по уголовным делам Первого кассационного суда общей юрисдикции от 18 ноября 2021 г. приговор и апелляционное определение в отношении Н. оставлены без изменения.

В кассационном представлении заместитель Генерального прокурора Российской Федерации просил об отмене вынесенных по уголовному делу в отношении Н. судебных решений, оспаривая выводы об отсутствии доказательств того, что Н., размещая видеоролики порнографического содержания на своей странице в социальной сети, стремился к их распространению, а не преследовал цель личного их использования. Автор представления указывал, что, разместив на своей странице в социальной сети «ВКонтакте» соответствующие видеозаписи и не запретив доступ другим пользователям социальной сети как к своей странице, так и к скопированным видеофайлам, Н. тем самым умышленно распространил материалы с порнографическими изображениями несовершеннолетних, поскольку создал условия, обеспечивающие свободный доступ неопределенному кругу лиц к указанным материалам, и предоставил им возможность для дальнейшего копирования видеофайлов. Ссылался также на то, что страница Н. в социальной сети в открытом доступе имеет 65 «друзей», 97 подписчиков и 18 видеозаписей.

Как следует из материалов уголовного дела, органами предварительного следствия Н. обвинялся в том, что, обладая знаниями в области информационных технологий и навыками пользователя компьютерной техникой, посредством мобильного телефона с функцией доступа к информационно-телекоммуникационной сети «Интернет» в один

из дней в период с 2017 по 2019 г. вступил в одно из закрытых сообществ в социальной сети «ВКонтакте», где получил доступ к материалам с порнографическими изображениями малолетних и несовершеннолетних. Используя ранее зарегистрированный аккаунт под именем «Д.Р.», он осуществил распространение этих материалов, умышленно предоставляя другим пользователям сети «Интернет», материалы с порнографическим изображением лиц, не достигших 14-летнего возраста, разместив на своей странице в общем доступе видеозаписи под названиями, однозначно свидетельствующими о том, что на них содержатся порнографические изображения малолетних.

Лискинский районный суд Воронежской области, признав доказанным размещение Н. на своей странице в социальной сети «ВКонтакте» двух видеороликов с порнографическими изображениями несовершеннолетних лиц, не достигших 16 лет, и оправдывая Н. по обвинению в совершении преступления, предусмотренного п. «г» ч. 2 ст. 242^1 УК РФ, за отсутствием в указанных действиях состава преступления, исходил из того, что достаточных доказательств, подтверждающих распространение Н. каким-либо способом порнографических материалов с изображениями несовершеннолетних, не представлено, а его показания о размещении указанных материалов на собственной странице для удовлетворения личных сексуальных интересов ничем не опровергнуты. Отвергая же доводы стороны обвинения, суд указал, что Н., добавляя (копируя) и храня файлы на своей странице, их никому не предлагал и не передавал, а само по себе добавление осужденным роликов к себе на страницу не свидетельствует об умысле на распространение информации; доказательств же, свидетельствующих о том, что видеофайлы с порнографическими изображениями несовершеннолетних, не достигших 16-летнего возраста, были распространены Н., то есть получены другими лицами в результате его целенаправленных действий, в материалах уголовного дела не имеется.

Между тем в соответствии с принципом работы социальной сети «ВКонтакте» после размещения на странице пользователя видеозаписи у всех «друзей» и подписчиков в новостной ленте появляется сообщение о том, что пользователь добавил этот файл, и начинается его воспроизведение хотя и не в полноэкранном режиме, но с предоставлением возможности свободного открытия и просмотра.

Согласно составленному по результатам проведенного оперативно-розыскного мероприятия акту сбора образцов для сравнительного исследования от 7 марта 2019 г., принадлежащая Н. страница в социальной сети «ВКонтакте» под именем «Д.Р.», в открытом доступе имеет 65 «друзей», 97 подписчиков, 18 видеозаписей. Таким образом, суд не учел, что страница Н. в социальной сети, на которую он добавил видеоролики из закрытого сообщества, была открыта и любой пользователь мог ознакомиться с этими материалами, что нашло свое подтверждение в ходе проведения оперативно-розыскного мероприятия. Согласно упомянутому акту сбора образцов, одна из видеозаписей имела 169 199 просмотров, а вторая - 238 816 просмотров в социальной сети. Каких-либо действий, направленных на ограничение или запрет доступа сторонних лиц на его страницу с размещенными на ней видеороликами, Н. не совершал.

Ссылка же суда на неосведомленность Н. об автоматическом размещении добавленных им на свою страницу видеофайлов в новостной ленте «друзей» и о возможности их свободного просмотра является несостоятельной, поскольку, регистрируясь в социальной сети, Н. был ознакомлен с Правилами пользования сайтом «ВКонтакте», без отметки о чем регистрация на этом сайте невозможна.

Кроме того, давая юридическую оценку действиям Н., суд не учел, что согласно диспозиции статьи 242^1 УК РФ инкриминируемое осужденному преступление не предполагает в качестве обязательного признака фактический просмотр кем-либо из посетителей страницы с размещенным на ней порнографическим сайтом; достаточно того, что, размещая в социальной

сети «ВКонтакте» такой сайт, осужденный исходил из того, что он может быть просмотрен неопределенным кругом лиц. Такое толкование нормы ч. 1 ст. 242[1] УК РФ находит подтверждение, в частности, в положении п. 9 ст. 2 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации», согласно которому под распространением информации понимаются действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц.

При таких обстоятельствах Судебная коллегия по уголовным делам Верховного Суда пришла к выводу о том, что решения судов первой, второй и кассационной инстанций в отношении Н. об отсутствии в его действиях состава преступления не подтверждаются фактическими обстоятельствами уголовного дела и не соответствуют положениям уголовного закона. Допущенные судом нарушения уголовного закона повлияли на исход уголовного дела и повлекли безосновательное освобождение лица, для вывода о невиновности которого в совершении преступления не имеется оснований, от уголовной ответственности, что искажает саму суть правосудия и смысл судебного решения как акта правосудия.

Судебная коллегия определила: отменить приговор и последующие судебные решения, уголовное дело передать в тот же суд первой инстанции на новое судебное рассмотрение иным составом суда.

12. Совершенные обвиняемым действия по скачиванию и хранению видеоролика порнографического содержания на своем персональном компьютере сами по себе не позволяют сделать бесспорный вывод о наличии у него умысла на его распространение[49].

По приговору Керченского городского суда Республики Крым от 23 марта 2021 года М. осужден по п. п. «а», «г» ч. 2 ст. 242[1] УК РФ к 3 годам

[49] Определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 04.08.2022 № 127-УД22-12-К4 // СПС «КонсультантПлюс» (дата обращения: 31.07.2023).

лишения свободы в соответствии со ст. 73 УК РФ условно, с испытательным сроком на 6 месяцев.

В апелляционном порядке указанный приговор не обжалован и вступил в законную силу 5 апреля 2021 года.

Кассационным определением судебной коллегии по уголовным делам Четвертого кассационного суда общей юрисдикции от 8 декабря 2021 года обвинительный приговор в отношении М. отменен.

Уголовное дело в отношении М. прекращено на основании п. 2 ч. 1 ст. 24 УПК РФ за отсутствием в деянии состава преступления.

Признано за М. право на реабилитацию.

В кассационном представлении заместитель Генерального прокурора Российской Федерации поставлен вопрос об отмене кассационного определения судебной коллегии по уголовным делам Четвертого кассационного суда общей юрисдикции от 8 декабря 2021 года, направлении уголовного дела на новое кассационное рассмотрение.

По доводам представления при рассмотрении уголовного дела в кассационном порядке были допущены повлиявшие на исход дела нарушения закона, исказившие саму суть правосудия и смысл судебного решения как акта правосудия.

Проверив материалы дела, обсудив доводы кассационного представления, Судебная коллегия не находит оснований для отмены кассационного определения.

Признавая М. виновным в приобретении, хранении в целях распространения, а также распространении материалов с порнографическими изображениями несовершеннолетних, в отношении лица, не достигшего 14-летнего возраста с использованием информационно-телекоммуникационной сети «Интернет», судом было установлено, что М., имея в собственности переносной персональный компьютер с целью распространения порнографических материалов, в том числе с изображением несовершеннолетних, не достигших четырнадцатилетнего возраста,

используя сеть «Интернет», установил на жесткий магнитный диск программное обеспечение. Далее с целью обмена различными файлами при подключении к файлообменной сети посредством программного обеспечения при его установке определил для скачивания файлов адрес, осознавая, что файлы, помещенные в указанный каталог, будут доступны для скачивания с целью просмотра другим пользователям файлообменной сети посредством программного обеспечения. После чего с целью последующего распространения загрузил и хранил по адресу видеофайл, содержащий изображения полностью обнаженных половых органов и полового сношения несовершеннолетних лиц, в том числе не достигших четырнадцатилетнего возраста, чем целенаправленно предоставил возможность неограниченному кругу лиц в сети «Интернет» для свободного копирования и просмотра указанного видеофайла.

При этом суд как на доказательство виновности М., сослался на его показания данные в ходе предварительного следствия в качестве подозреваемого в присутствии защитника, из которых следует, что в начале марта он скачал на свой компьютер компьютерную программу, предназначенную для обмена файлами по электронным пиринговым сетям сети «Интернет». При установлении на компьютерном оборудовании программа автоматически формирует хранилище – папки, в которые сохраняется вся скопированная пользователем информация, то есть он прекрасно понимал, что сохраненная информация на его ноутбуке будет доступна неограниченному кругу лиц в сети «Интернет» для свободного просмотра и скачивания. В начале марта он, используя эту программу, скачал на свой ноутбук видеоролик порнографического содержания. Указанный видеоролик удалил, так как он был ему неинтересен. Как таковой цели распространения данного видеоролика он не преследовал.

Между тем, показания М. об удалении видеоролика не опровергнуты представленными стороной обвинения и исследованными в судебном заседании доказательствами. На изъятых в ходе осмотра квартиры

осужденного компьютерах не обнаружено ни видеоролика, который он скачал, ни иных материалов порнографического содержания.

В судебном заседании М. пояснил, что не помнит точно, когда скачал видеоролик и когда его удалил, этот видеоролик неинтересен ему был ни для хранения, ни для распространения.

Принимая во внимание то обстоятельство, что удаление видеоролика исключало доступ к нему как самого М., так и иных лиц, показания в судебном заседании М., который отрицал наличие у него умысла на распространение порнографических материалов, Судебная коллегия находит обоснованным вывод суда кассационной инстанции об отсутствии доказательств, свидетельствующих о том, что М. совершил действия, направленные на распространение видеоролика порнографического содержания, что стороной обвинения не было представлено каких-либо доказательств того, что М. предлагал или передавал иным лицам скачанный им видеофайл.

Судебная коллегия определила: определение судебной коллегии по уголовным делам Четвертого кассационного суда общей юрисдикции от 8 декабря 2021 года в отношении М. оставить без изменения, кассационное представление заместителя Генерального прокурора Российской Федерации Т. – без удовлетворения.

13. Ссылка в жалобе на то, что отдельные материалы террористического и экстремистского содержания, размещенные в сети «Интернет», не были изготовлены самим осужденным, не влияет на правильность вывода суда относительно направленности его умысла при совершении преступлений[50].

По приговору Центрального окружного военного суда от 21 апреля 2022 г. Ш. осужден к лишению свободы: по ч. 2 ст. 205^2 УК РФ за совершение пяти преступлений на срок 5 лет с лишением права заниматься

[50] Кассационное определение Судебной коллегии по делам военнослужащих Верховного Суда Российской Федерации от 22.03.2023 № 223-УД23-4-А6 // СПС «КонсультантПлюс» (дата обращения: 15.08.2023).

деятельностью, связанной с администрированием сайтов и каналов с использованием электронных и информационно-телекоммуникационных сетей, в том числе сети «Интернет», на срок 3 года, за каждое; по ч. 2 ст. 280 УК РФ за совершение трех преступлений на срок 3 года с лишением права заниматься деятельностью, связанной с администрированием сайтов и каналов с использованием электронных и информационно-телекоммуникационных сетей, в том числе сети «Интернет», на срок 2 года, за каждое; по ч. 1 ст. 282 УК РФ на срок 2 года.

По совокупности преступлений на основании ч. 3 ст. 69 УК РФ путем частичного сложения наказаний Ш. окончательное наказание назначено в виде лишения свободы на срок 6 лет в исправительной колонии общего режима с лишением права заниматься деятельностью, связанной с администрированием сайтов и каналов с использованием электронных и информационно-телекоммуникационных сетей, в том числе сети «Интернет», на срок 4 года.

Апелляционным определением апелляционного военного суда от 16 августа 2022 г. приговор в отношении Ш. оставлен без изменения.

Ш. признан виновным и осужден за то, что он, испытывая неприязнь к органам государственной власти и правоохранительным органам, используя устройство, имеющее выход в информационно-телекоммуникационную сеть «Интернет» (далее – сеть «Интернет»), с целью доведения до неопределенного круга лиц информации, призывающей к террористической и экстремистской деятельности, путем размещения в свободном доступе в социальной сети указанных в приговоре материалов, совершил:

- 14, 17 октября 2017 г., 21 марта, 2 октября 2018 г., а также 3 августа 2019 г. публичные призывы к осуществлению террористической деятельности;

- 9, 14 октября 2017 г., а также в период с 24 декабря 2019 г. по 7 января 2020 г. публичные призывы к осуществлению экстремистской деятельности.

Кроме того, 12 марта 2020 г. в связи с негативным отношением к представителям одной национальности Ш. таким же способом совершил публичные действия, направленные на возбуждение ненависти и вражды в отношении группы лиц, выделенной по признаку национальности, будучи привлеченным к административной ответственности за аналогичное деяние в течение одного года.

Адвокат в кассационной жалобе указывает, что приговор и апелляционное определение в отношении Ш. являются незаконными, необоснованными и подлежащими отмене в связи с несоответствием выводов суда фактическим обстоятельствам уголовного дела, существенным нарушением уголовно-процессуального закона, неправильным применением уголовного закона и несправедливостью приговора. Ссылается на то, что персональную страницу на сайте социальной сети Ш. создал для личного пользования, размещенные материалы (видеоролики и посты) ему не принадлежали и не предназначались для демонстрации иным лицам, он никого не призывал к их просмотру. Отмеченные как понравившиеся материалы отображались в ленте активности его профиля автоматически. Адвокат просит приговор и апелляционное определение отменить, уголовное дело направить на новое рассмотрение в суд первой инстанции.

В возражениях на апелляционную жалобу заместитель прокурора Самарской области просит об оставлении приговора и апелляционного определения без изменения, а кассационной жалобы без удовлетворения.

Проверив материалы уголовного дела, обсудив доводы кассационной жалобы, выслушав стороны, Судебная коллегия по делам военнослужащих Верховного Суда Российской Федерации приходит к следующим выводам.

Действия Ш. по опубликованию в сети «Интернет» информации террористической и экстремистской направленности осуществлялись им на регулярной основе в период с 2017 по 2020 годы. Размещенные материалы имели многочисленные просмотры. Пользовательской аудитории доводились не только заимствованные Ш. текстовые сообщения, но и соответствующие

видеоматериалы, фотоизображения и ссылки на них, а также собственные комментарии Ш., что усиливало негативное воздействие распространяемой им информации.

Так, материалы, опубликованные 24 декабря 2019 г., 3 и 7 января 2020 г., представляли собой текстовые комментарии, в том числе самого Ш., видеоролик, побуждающий к действиям насильственного характера и ссылку на него, а материал, размещенный 14 октября 2017 г., содержал текстовое сообщение и фотоизображение с призывами к насильственному изменению конституционного строя Российской Федерации.

Материал, направленный на возбуждение ненависти, вражды в отношении группы лиц, выделенной по признаку национальности, распространен Ш. в сети «Интернет», несмотря на его привлечение к административной ответственности за аналогичные действия.

Информация, адресованная Ш. пользователям социальных сетей, понимавших ее террористическую и экстремистскую направленность, побуждала их выражать в комментариях свое отношение к ней, что осознавалось Ш.

При таких обстоятельствах ссылка в жалобе на то, что отдельные материалы, размещенные в сети «Интернет», не были изготовлены самим Ш., не влияет на правильность вывода суда относительно направленности его умысла при совершении преступлений.

Судебная коллегия определила: приговор Центрального окружного военного суда от 21 апреля 2022 г. и апелляционное определение апелляционного военного суда от 16 августа 2022 г. в отношении Ш. изменить. Считать, что за совершенные 14 и 17 октября 2017 г. с использованием сети «Интернет» публичные призывы к осуществлению террористической деятельности Ш. осужден по ч. 2 ст. 205^2 УК РФ (в редакции Федерального закона от 6 июля 2016 г. № 375-ФЗ) за каждое преступление.

В остальном приговор и апелляционное определение в отношении Ш. оставить без изменения, а кассационную жалобу адвоката без удовлетворения.

14. Суд опроверг доводы стороны защиты о неверной квалификации действий осужденных. Все преступления, совершенные осужденными, являются оконченными, поскольку каждый раз при неправомерном доступе к охраняемой законом компьютерной информации, эта информация была скопирована; сведения, составляющие банковскую тайну, которые были доверены одному из подсудимых по службе, без согласия владельца были незаконно разглашены, объективная сторона преступлений осужденными была выполнена[51].

Приговором Кировского районного суда г. Ярославля от 25 ноября 2021 года ФИО1 осужден за пять преступлений, каждое их которых предусмотрено ч. 3 ст. 272 УК РФ, к 4 месяцам лишения свободы за каждое. В соответствии с ч. 2 ст. 69 УК РФ по совокупности преступлений путем частичного сложения назначенных наказаний назначено наказание в виде 7 месяцев лишения свободы.

ФИО2 осужден за четыре преступления, каждое их которых предусмотрено ч. 3 ст. 272 УК РФ, к 4 месяцам лишения свободы за каждое. В соответствии с ч. 2 ст. 69 УК РФ по совокупности преступлений путем частичного сложения назначенных наказаний назначено наказание в виде 6 месяцев лишения свободы.

ФИО3 осужден за два преступления, каждое из которых предусмотрено ч. 3 ст. 272 УК РФ, два преступления, каждое из которых предусмотрено ч. 3 ст. 183 УК РФ, к 4 месяцам лишения свободы за каждое. В соответствии с ч. 2 ст. 69 УК РФ по совокупности преступлений путем частичного сложения

[51] Апелляционное постановление № 22-145/2022 от 02.02.2022 по делу № 1-59/2021 // URL: https://sudact.ru/regular/doc/gZ8MVbNHN3H/?regular-txt=&regular-case_doc=&regular-lawchunkinfo=Статья+272.+Неправомерный+доступ+к+компьютерной+информации%28УК+РФ%29&regular-date_from=&regular-date_to=&regular-workflow_stage=&regular-area=&regular-court=&regular-judge=&_=1692182310260 (дата обращения: 16.08.2023).

назначенных наказаний назначено наказание в виде 6 месяцев лишения свободы.

В апелляционной жалобе адвокаты в защиту интересов ФИО1, ФИО2, ФИО3 выражают несогласие с приговором, считая его необоснованным и несправедливым.

По мнению защитника, действия ФИО1 надлежало квалифицировать как единое продолжаемое преступление, которое не было доведено до конца, то есть по ч. 3 ст. 30 и ч. 3 ст. 272 УК РФ. В обоснование своей позиции указывает, что все 5 тождественных преступлений, объединенных единым умыслом, квалифицированных по ч. 3 ст. 272 УК РФ, проходили в рамках оперативно-розыскного мероприятия «оперативный эксперимент», где в роли мнимого покупателя выступал сотрудник УФСБ России по Ярославской области, который переводил денежные средства на Киви кошелек, к нему же поступали фотоизображения, содержащие информацию о движении денежных средств по банковской карте, сведения о владельцах абонентского номера ПАО «Вымпелком», АО «РТК», ПАО «МТС», а также компьютерная информация со сведениями о доходах физического лица. Указанные обстоятельства, как считает автор жалобы, свидетельствуют о том, что охраняемая законом компьютерная информация не поступила гражданам для неправомерного использования, следовательно, неправомерного доступа к компьютерной информации не произошло.

В апелляционной жалобе адвокат ФИО3 ставит вопрос об изменении приговора в отношении своего подзащитного. Полагает, что тождественные действия ФИО3, охваченные единым умыслом, которые контролировались сотрудниками ФСБ, должны быть квалифицированы как неоконченное продолжаемое преступление.

В апелляционной жалобе адвокат ФИО2 выражает несогласие с судебным решением в отношении своего подзащитного. Считает, что все преступления, вменяемые ФИО2, не были доведены до конца по независящим от него основаниям, поскольку находились под контролем

оперативных сотрудников, информация, передаваемая ФИО2, не поступила гражданам для использования, неправомерного доступа к охраняемой законом компьютерной информации, повлекшей уничтожение, блокирование, модификацию либо копирование компьютерной информации, не произошло.

На апелляционные жалобы защитников осужденных государственным обвинителем принесены возражения, в которых указано на необоснованность изложенных в них доводов.

Выслушав участников процесса, проверив доводы апелляционных жалоб, суд апелляционной инстанции не находит оснований для удовлетворения апелляционных жалоб.

Суд правильно исходил из того, что из предъявленного обвинения, с которым согласились осужденные, следует, что каждое преступление было совершено каждый раз с новым умыслом, возникновение которого предопределялось вновь создававшимися условиями, в том числе обращением лица, желающего получить информацию, составляющую банковскую тайну - клиента, при различных обстоятельствах, в разное время, в отношении различных объектов преступного посягательства. В соответствии с ч. 1 ст. 17 УК РФ суд верно оценил действия осужденных как совокупность преступлений.

Все преступления являются оконченными, поскольку каждый раз при неправомерном доступе к охраняемой законом компьютерной информации, эта информация была скопирована; сведения, составляющие банковскую тайну, которые были доверены одному из подсудимых по службе, без согласия владельца были незаконно разглашены, объективная сторона преступлений осужденными была выполнена. Документирование преступной деятельности осужденных посредством проведения оперативно-розыскных мероприятий не указывает, что имело место покушение на преступления.

Суд постановил: приговор Кировского районного суда г. Ярославля от 25 ноября 2021 года в отношении ФИО1, ФИО2 и ФИО3 оставить без изменения, а апелляционные жалобы защитников – без удовлетворения.

15. В качестве охраняемой законом компьютерной информации рассматривается как информация, для которой законом установлен специальный режим правовой защиты, так и информация, для которой обладателем информации установлены средства защиты, направленные на обеспечение ее целостности и (или) доступности[52].

По приговору Белокалитвинского городского суда Ростовской области от 25 января 2023 года Т. признан виновным в совершении преступлений, предусмотренных ч. 3 ст. 272, ч. 3 ст. 272 УК РФ, с назначением ему наказания: по ч. 3 ст. 272 УК РФ (эпизод с 30.09.2021 г. по 07.10.2021 г.) в виде 1 года 6 месяцев лишения свободы, по ч. 3 ст. 272 УК РФ (эпизод с 08.10.2021 г. по 13.10.2021 г.) в виде 1 года 6 месяцев лишения свободы; на основании ч. 2 ст. 69 УК РФ по совокупности преступлений, путем частичного сложения назначенных наказаний, окончательно назначено наказание в виде 1 года 8 месяцев лишения свободы; на основании ст. 73 УК РФ назначенное наказание считается условным, с испытательным сроком 2 года.

Так, Т. признан виновным в совершении двух эпизодов по неправомерному доступу к охраняемой законом компьютерной информации, если это деяние повлекло копирование компьютерной информации, совершенное группой лиц по предварительному сговору, в период с 30.09.2021 по 07.10.2021, с 08.10.2021 по 13.10.2021.

В апелляционной жалобе защитник осуждённого ставит вопрос об отмене приговора, как незаконного и необоснованного и вынесении по делу оправдательного приговора в отношении Т. Указывает, что в результате действий Т. существенный вред никому причинён не был, потерпевшие с

[52] Апелляционное постановление от 06.04.2023 по делу № 22-1867/2023 // URL: https://судебныерешения.рф/74648335 (дата обращения: 16.08.2023).

заявлениями в правоохранительные органы не обращались, как именно и кем была использована информация, не установлено.

На вышеуказанную апелляционную жалобу государственным обвинителем поданы возражения, из которых усматривается, что обжалуемый приговор необходимо оставить без изменения, апелляционную жалобу защитника – без удовлетворения.

Изучив материалы уголовного дела, суд апелляционной инстанции приходит к следующим выводам.

Доводы апелляционной жалобы о невиновности Т. опровергаются совокупностью доказательств по делу, приведенных в обжалуемом приговоре, с которыми соглашается суд апелляционной инстанции.

В соответствии с ч. 1 ст. 53 Федерального закона от 07.07.2003 № 126-ФЗ «О связи» сведения об абонентах и оказываемых им услугах связи, ставшие известными операторам связи в силу исполнения договора об оказании услуг связи, являются информацией ограниченного доступа и подлежат защите в соответствии с законодательством Российской Федерации.

Исходя из пункта 1 примечаний к ст. 272 УК РФ под компьютерной информацией понимаются любые сведения (сообщения, данные), представленные в виде электрических сигналов, независимо от средств их хранения, обработки и передачи.

При этом в качестве охраняемой законом компьютерной информации рассматривается как информация, для которой законом установлен специальный режим правовой защиты, ограничен доступ, установлены условия отнесения ее к сведениям, составляющим государственную, коммерческую, служебную, личную, семейную или иную тайну (в том числе персональные данные), установлена обязательность соблюдения конфиденциальности такой информации и ответственность за ее разглашение, так и информация, для которой обладателем информации

установлены средства защиты, направленные на обеспечение ее целостности и (или) доступности.

В соответствии с разъяснениями, содержащимися в п. 4 Постановления Пленума Верховного Суда РФ от 15.12.2022 № 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» под копированием компьютерной информации понимается 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.).

Применительно к ст. 272 УК РФ неправомерным доступом к компьютерной информации является получение или использование такой информации без согласия обладателя информации лицом, не наделенным необходимыми для этого полномочиями, либо в нарушение установленного нормативными правовыми актами порядка независимо от формы такого доступа (путем проникновения к источнику хранения информации в компьютерном устройстве, принадлежащем другому лицу, непосредственно либо путем удаленного доступа).

Так, на основе исследованных доказательств в суде первой инстанции установлено, что в период с 30.09.2021 по 07.10.2021 действиями Т., Ч., приговор в отношении которой не обжалуется, и неустановленного лица охраняемая законом компьютерная информация с персональными данными абонентов ПАО «МТС» была разглашена третьим лицам, не имеющим к ней свободного доступа на законных основаниях.

Суд постановил: приговор Белокалитвинского городского суда Ростовской области от 25 января 2023 года в отношении Т. – оставить без

изменения, апелляционную жалобу защитника осуждённого – без удовлетворения.

5. Противодействия расследованию киберпреступлений и его преодоление

Проблема противодействия расследованию приобрела в последнее время особенную актуальность и остроту в связи с широким распространением киберпреступности. По отношению к процессу расследования конкретного преступления следует различать «внутреннее» и «внешнее» противодействие.

Под внутренним противодействием понимают противодействие, оказываемое теми или иными лицами, причастными в любой форме к расследованию: подозреваемыми и обвиняемыми, свидетелями и потерпевшими, специалистами и экспертами, случайными лицами, оказавшимися на месте происшествия, и др. Для них характерно обладание какой-то информацией о событии и стремление скрыть, изменить или уничтожить эту информацию и (или) ее носителей. Внешнее противодействие — это противодействующая деятельность лиц, либо вообще не связанных с расследуемым событием и лицом, осуществляющим расследование, либо связанных со следователем (дознавателем) процессуальными, служебными или иными властными отношениями или другими зависимостями. Нередки случаи, когда способ сокрытия компьютерных преступлений существует самостоятельно и не охватывается единым преступным замыслом. Противодействие расследованию осуществляется различными способами сокрытия. Это может быть утаивание информации или ее носителей как в активной, так и в пассивной формах; уничтожение полное или частичное; фальсификация; маскировка способа преступления, личности преступника; инсценировка и комбинации этих способов.

Противодействие расследованию компьютерных преступлений, как правило, не направлено против конкретного следователя, но на воспрепятствование обнаружению и расследованию самих компьютерных преступлений.

Для компьютерных преступлений субъекты внутреннего противодействия реализуют свои замыслы преимущественно путем сокрытия преступления. Субъекты внешнего противодействия компьютерных преступлений оказывают влияние на расследование созданием благоприятных условий для совершения противозаконных действий, а также непониманием ценности предоставленной в их распоряжение компьютерной информации, беспечностью и отсутствием ответственного отношения к возможным негативным последствиям своих необдуманных действий, боязнью порицания за несанкционированный доступ к компьютерной информации и т.п.

Основываясь на методологии криминалистики, включающей методы диалектической и формальной логики, общенаучные и специальные методы, с учетом анализа следственной и оперативно-розыскной практики приходим к выводу о необходимости изменения сложившихся стереотипов, связанных с традиционными методами преодоления противодействию расследования, поскольку способы компьютерных преступлений не коррелируют напрямую с их видами, а для совершения разных видов компьютерных преступлений часто используются одни и те же методы и информационно-компьютерное обеспечение. Остановимся в этой связи на современных проблемах криминалистических методик, позволяющих осуществить эффективное преодоление противодействию расследования. Основу любой криминалистической методики составляет криминалистическая характеристика преступлений, базирующаяся на типовой информационной модели. Моделирование производится путем обобщения сведений о криминалистически значимых признаках вида преступления, полученных из

массивов уголовных дел, и прослеживания закономерных связей между этими признаками.

Представляет интерес исследование А.А. Бессонова, где произведено, обобщение двух вышеупомянутых категорий и сделан вывод, что «Криминалистическая характеристика преступлений… информационная модель, которая отражает криминалистическую сущность преступлений определённого вида (подвида, криминалистически схожих групп), заключающуюся в сведениях о его криминалистически значимых признаках и их закономерных связях между собой, построенная на основе анализа и обобщения практики их расследования и судебного рассмотрения, и имеющая значение для формирования частных методик расследования и решения задач деятельности по расследованию и предупреждению преступлений» .

Процессы цифровизации обусловили начало активного внедрение IT-технологии в сферу уголовного судопроизводства, что открывает возможности обобщения больших массивов криминалистки значимой информации. Базируясь на подходе к криминалистической характеристике вида преступления как к информационной модели А.А. Бессонов выступил предложением: «создавать цифровые модели, максимально адаптированные к использованию в цифровой среде…по сути речь идет о цифровизации типовых криминалистических характеристик преступлений, т.е. о представлении их в форме соответствующих цифровых моделей».

Но, как указывалось выше, различные виды преступлений с использованием компьютерных средств и систем, могут совершаться одним и тем же способом. В качестве примера рассмотрим один из способов обеспечения преступником анонимности своих действий в сети Интернет с использованием цепочки прокси-серверов. VPN-технологии обеспечивают шифрование сетевого трафика между компьютером пользователя и VPN-прокси-сервером, являющимся шлюзом выхода в сеть Интернет и, соответственно, скрывают реальный IP-адрес пользователя. Если необходим

более высокий уровень конспирации, преступники арендуют вычислительные мощности у провайдеров хостинговых услуг в любой точке мира и настраивают на них собственные VPN-серверы или виртуальные машины.

Способы компьютерных преступлений, как мы отмечали выше, являются полноструктурными, причем могут быть выбраны различные технологии подготовки, совершения и сокрытия, слабо коррелирующие с видом преступления. Отметим, что в большинстве современных программ-троянов сочетаются целые наборы функций, открывающие преступникам широкие возможности для манипулирования пользовательской информацией. Например, Trojan-Banker.Win32.RTM, помимо присущей только этому виду троянских программ функциональности поиска и копирования пользовательской информации, относящейся к банковским счетам, системам электронных денег и пластиковым картам, обладает возможностями:

- поиска файлов по именам,
- записи истории нажатий клавиш клавиатуры,
- записи видео и создании снимков экрана,
- копирования буфера обмена,
- блокирования и нарушения работы операционной системы,
- получения от сервера управления команд на запуск дополнительных программных модулей, отправки собранной информации на сервер управления и т.п.

Именно поэтому объединение информационных моделей по видам преступлений не является результативным. Общность способов компьютерных преступлений начала прослеживаться еще в конце XX века, хотя тогда информационные технологии в нашей стране еще мало использовались в преступной деятельности.

Основой для нашего исследования, как отмечалось выше, послужила криминалистическая методология, а также мониторинг следственной и

оперативно-розыскной практики, результаты опросов и анкетирования специалистов в области IT-технологий. Эти опросы показали, что сегодня необходимы новые подходы к расследованию компьютерных преступлений, поскольку их способы не находятся в прямой зависимости от видов этих преступлений. Для подготовки, совершения и сокрытия как преступлений в сфере компьютерной информации (Глава 28 УК РФ), так и других видов преступлений, например, краж, мошенничеств, убийств, создания групп смерти, организации массовых беспорядков и террористических актов, незаконного оборота наркотических средств, преступлений в банковской сфере, незаконной организации азартных игр и других используется зачастую одно и то же информационно-компьютерное обеспечение преступной деятельности.

Родовая криминалистическая характеристика компьютерных преступлений обусловливает общность способов преступлений в пределах данного криминалистического рода. А для преступлений, совершаемых «традиционными» способами, элементы криминалистической характеристики тесно связаны с видом преступления, поэтому можно констатировать для разных видов преступлений различия во всех элементах их криминалистических характеристик. В этом и состоит особенность компьютерных преступлений.

Для создания методик расследования компьютерных преступлений необходимо изменить подход к отбору и систематизации криминалистически значимых признаков преступлений. В этих условиях необходимо формировать типовые информационные модели, которые могут приобрести уже совершенно новое звучание, будучи основаны на использовании современных информационно-компьютерных технологиях. На основании общности способов для различных видов преступлений, совершаемых с использование компьютерных средств и систем, возможно формирование информационно-компьютерных моделей преступлений, которые будут отличаться предметами посягательства и, в какой-то степени, потерпевшей

стороной. Что касается сведений о личности типичного преступника, то, в первую очередь, важна информация о том, каков его уровень владения компьютерными технологиями. Основу характеристики потерпевшего (потерпевшей стороны) также должна составлять его компетенция в области IT-технологий.

Основным принципом формирования информационно-компьютерных моделей является ранжирование их по сложности способов реализации противоправных действий, включая используемые IT-технологии и корреляции с этими способами уровня компетенции преступников, состава преступной группы или сообщества.

Корреляционные связи существуют также между способом компьютерного преступления и компьютерной грамотностью потерпевшего, которая также может иметь разные уровни по компетентности: пользователь; специалист в области IT-технологий.

Приведем несколько примеров. Для несанкционированного доступа к компьютерным средствам и системам одним из основных способов является внедрение троянских программ при массовых рассылках сообщений электронной почты, содержащих вложения, маскирующиеся под полезный для пользователя документ, так называемых фишинговых писем (от англ. fish – ловить рыбу). При попытке открытия такого вложения в систему загружается и устанавливается троянская программ. Иначе этот способ реализуется не через вложение, а через интернет-ссылку, при переходе по которой неопытный пользователь направляется на сайт, содержащий наборы программ, которые находят слабые места в безопасности компьютерной системы и через них загружают вредоносную программу. Данный способ распространения вредоносного программного обеспечения настолько востребован, что пользователям постоянно советуют не открывать неизвестных вложений и не переходить, но неизвестным ссылкам, прикрепленным к электронным письмам. Использование этого способа дает представление об уровне компетенции как преступника, так и потерпевшего.

Значительно более сложными являются способы, которые построены на модульной архитектуре, когда дополнительный модуль отвечает за конкретный вид действия, но на зараженном компьютере может работать только во взаимодействии с главным модулем. Информацию о компьютерной системе, собранную основным модулем пользователя, программа направляет на управляющий сервер, который отдает команду по загрузке на компьютер дополнительных модулей, необходимых для реализации преступного умысла. Это позволяет атаковать не только компьютеры физических лиц, но крупные корпоративные сети, например, для хищения денежных средств либо кражу конфиденциальной информации.

Очевидно, что для подготовки, совершения и сокрытия подобных преступлений необходимо участие группы или сообщества, обладающих высоким уровнем компетенции в области IT-технологий. Потерпевшая сторона здесь будет представлена значительно более квалифицированными пользователями или системными администраторами.

Другим примером являются компьютерные атаки на локальные корпоративные сети. Эти атаки могут быть как внешними, так и производиться изнутри организации с участием ее сотрудников. Заметим, что преступник-инсайдер может использовать вредоносные программы, как и преступник-аутсайдер. Причем его участие может быть опосредованным путем предоставления соучастникам сведений, необходимых для несанкционированного доступа к корпоративной компьютерной сети, в том числе об уязвимых местах в программном обеспечении или либо ошибках в настройках сетевого оборудования.

В ряде случаях необходимым условием является вовлечение потерпевшего в преступление путем прямого общения с применением психологических приемов, склоняющих, например, к разглашению уникального кода в СМС-сообщении для авторизации на сетевом ресурсе, или к самостоятельной загрузке программы удаленного администрирования

на свой компьютер и предоставлению реквизитов доступа к нему преступникам.

Важно иметь в виду, что недостаточная компетенция пользователей и связанный с этим низкий уровень обеспечения информационной безопасности, в том числе использование ненадежных паролей, заводских настроек и конфигураций программного обеспечения и оборудования предоставляет широкий спектр возможностей для получения несанкционированного доступа к конфиденциальной информации.

На основе учения об информационно-компьютерных криминалистических моделях компьютерных преступлений используя технологии больших данных (Big Data) можно начать разработку упомянутых А.А. Бессоновым цифровых криминалистических моделей видов компьютерных преступлений.

Использование информационно-компьютерных криминалистических моделей компьютерных преступлений в преодолении противодействия расследованию на примере «кибершантажа»

Рассмотрим использование информационно-компьютерных моделей, сформированных по принципу их ранжирования в зависимости от сложности способов реализации противоправных действий, включая используемые IT-технологии и корреляции уровня компетенции преступников, состава преступной группы или сообщества с этими способами на примере расследования одного из быстро распространяющихся и постоянно модифицирующихся видов преступлений – вымогательства с использованием сети Интернет. Проблема «кибершантажа» имеет транснациональный характер и ей в зарубежной литературе уделяется достаточно большое внимание, где данное явление приобрело наименование – ransomware. Однако следует подчеркнуть, что данный вопрос в основном рассматривается с точки зрения обеспечения информационной безопасности (Information Security). В криминалистическом и криминологическом аспектах эта проблема пока мало разработана, хотя его жертвами становятся не только

физические, но и юридические лица. По данным Лаборатории Касперского 4596 вредоносных пакетов оказались мобильными троянцами-вымогателями только в первом квартале 2022 г. Нижняя граница суммарного ущерба от действий программ-вымогателей, по оценкам Group-IB, составляет более $1 млрд .

«Кибершантаж» – это противоправно действие, которое охватывает диспозиции сразу нескольких статей УК РФ (ст.ст.163, 137, 183, 272, 273 и др.). Основным объектом данного преступления являются имущественные права физических и/или юридических лиц. Однако по совокупности правонарушений дополнительным объектом будут: неприкосновенность тайны личной жизни, коммерческой, банковской и налоговой тайны; общественные отношения по безопасному использованию компьютерных средств и сетей. Расследование данных видов преступлений представляет сложность в основном из-за использования в процессе их совершения компьютерных средств и сетей, что влечет за собой большие проблемы в установлении места совершения преступления и лица его совершившего.

Начнем с рассмотрения преступлений в отношении физических лиц. Наиболее распространённой задачей преступников является получение информации о частной жизни путем внедрения в компьютерные средства и средства связи потерпевшего программного обеспечения, позволяющего: осуществлять запись, блокирование или перенаправление звонков, осуществляемых по средствам телефонии видеоконференций связи, мессенджеров; производить запись видео- и аудио- информации, используя внутренние средства компьютерного устройства; копировать данные из адресной книги телефона, почтовых программ и программ обмена сообщениями (мессенджеров); отправлять данные о местоположении; копировать данные; отправлять и получать SMS; отключать антивирусное программное обеспечение; просматривать историю браузера и выполнять иные функции. Получив сведения, компрометирующие потерпевшего или его близких, либо иные сведения, которые могут причинить существенный вред

правам или законным интересам потерпевшего или его близких, вымогатели предъявляют требования передачи им чужого имущества, чаще всего денежных средств путем перевода на указанные счета или путем отправления платных SMS сообщений. В последнее время получило распространение требования перевода на указанные электронные кошельки криптовалюты различных систем.

Под ударом находятся все пользователи сети Интернет, но наибольшую опасность такого рода преступления представляют для лиц, с невысоким уровнем компетенции в IT-технологиях либо склонных скачивать контент в обход официального производителя, а также увлекающихся компьютерными играми, поскольку именно при обновлениях, подобного программного обеспечения, покупки дополнительных функций, зачастую нелегальной, часто и происходит «заражение» компьютерного средства. Именно при распространения условно бесплатного программного обеспечения (ПО) имеется большое количество возможности вписать в распространяемый функционал необъявленную функцию, тем самым получив несанкционированный доступ к компьютерному средству. При поиске путей проникновения нелегального программного обеспечения на компьютерное средство необходимо анализировать именно пути «скачивания» обновлений, получения дополнительных функций и сами «скаченные» модули.

Изучением личности злоумышленника, свершающего вымогательство в отношении физических лиц с помощью угроз распространения, порочащих потерпевшего или близких ему людей сведений, установлено, что в настоящим момент это лица преимущественно мужского пола в возрасте от 18 до 30 лет, обладающие достаточно высоким уровнем компетенций в области компьютерных технологий. Но необходимо отметить, что постоянно возрастает процент женщин, вовлеченных в данный вид преступлений. Наши исследования показали, что в современных условиях нельзя акцентировать внимание только на лицах, хорошо владеющих IT-технологиями и навыками программирования, поскольку рынок программных продуктов очень широк и

сегодня производители вирусных программ и «троянов» предлагают разнообразное программное обеспечение, а покупателю такого продукта достаточно быть хорошим пользователем, способным самостоятельно разобраться в его применении. Хотя, конечно, это не отменяет необходимость для преступника владеть компетенциями в основах и принципах функционирования компьютерных средств и сети Интернет.

Другим способом осуществления компьютерного вымогательства является распространение программ-вымогателей, работающих по принципу «троянского коня». Целью действий этих программ является блокирование доступа пользователя к данным на компьютере или ограничение возможностей работы на компьютере и требование денежных средств за возврат к исходному состоянию системы. До недавнего времени подобного рода атаки совершались в основном на физических лиц, ярким примером этого может служить вредоносная программа, содержащая сообщение и изображение активиста Anonymous в маске и надпись «You have been Hacked» («Вас взломали»), текст на фарси с требованием оплаты выкупа в обмен на восстановление закодированных файлов. Мерой успешной борьбы, с ней мы предлагали предупреждения пользователям, что они должны просто игнорировать подобное предложение и не кликать на экране кнопку с надписью «Click Me» («Кликни на меня»). Теперь уровень компьютерной компетенции преступников вырос во много раз, а во всем мире потерпевшей стороной уже являются юридические лица: крупные корпорации и муниципальные информационные структуры. Ранее такие программы, чаще всего, вносили изменения в загрузочные модули программ, операционной системы и т.д., а сегодня – это уже шифрование данных. Если ранее специалисты по информационной безопасности организаций могли самостоятельно с использованием данных, полученных от организаций специализирующихся на написании антивирусных программ провести восстановление системы, то теперь в арсенал преступников вошли алгоритмы шифрования. Для декодирования информации, обработанной ими,

требуется знание и этих алгоритмов, и ключей к ним. Так недавно вымогатели начали использовать сложную гибридную комбинацию симметричного и асимметричного шифрования для кодирования файлов пользователей, подобрать ключ к которой практически невозможно. Изменился при данном способе вымогательства не только метод совершения преступления, но и метод передачи имущественных прав. Сегодня это практически всегда выражается в переводах на электронные счета кибервалюты.

Если говорить о потерпевшей стороне в преступлениях, совершаемых с использованием программ-вымогателей, то здесь следует отметить, что характеристика этих лиц претерпела существенные изменения. Конец 2020 года и весь 2021 год захлестнула волна программ-шифровальщиков, большинство вымогателей сфокусировались на атаках компаний коммерческого и государственного секторов. Всего за 2022 год публично известно о более чем 700 атаках, то есть практически имеет место «война», специалистов в области защиты информации и вымогателей. С обеих сторон фигуранты представлены специалистам высокого класса обладающими знаниями не только в области программирования и других IT-технологий, но высшей математики, и криптографии, что возможно только при наличии высшего образования не ниже уровня бакалавра. Соответственно возрастная группа таких преступников уже находится в диапазоне 25–45 лет, причем процент женщины имеет тенденцию к росту, что, на наш взгляд, объясняется популярностью образования в сфере IT-технологий.

При анализе цифровых следов, возникающие в результате проведения такого рода атак вымогателей, на наш взгляд, необходимо искать не только следы непосредственно «троянских» программ шифровальщиков, но и следы «программ разведчиков» – собирающих информацию о составе сетевой инфраструктуры предприятия и о его «чувствительных местах».

Следующим способом осуществления кибер-вымогательства является организация распределенных сетевых атак (DDoS атак), направленных на

блокирование доступа к сетевым ресурсам потерпевшего внешними пользователями. В основе таких атак лежит технологическое ограничение пропускной способности сетевой инфраструктуры, поддерживающей Интернет или телефонные ресурсы потерпевшего. Для DDoS атаки используют так называемые «ботнет-сети» – компьютерные сети с запущенными на устройствах ботами , которые управляются злоумышленниками удаленно. Киберпреступники активизируют запросы с помощью этих ботов, которые обращаются к сайту выбранной жертвы. Боднет-сети могут состоять как из зараженных устройств пользователей (например, компьютеров с активированными на них вирусами, которые хакеры используют без ведома пользователя), так и, например, из IoT-устройств: «умных» колонок, пылесосов и так далее .

Размер ботнета может составлять от десятков до сотен тысяч устройств. Во время таких атак в адрес сетевого-ресурса отправляется большое количество запросов с целью исчерпать его возможности обработки данных и нарушить нормальное функционирование. Если число запросов превышает предельные возможности хотя бы одного компонента сетевой инфраструктуры, могут возникнуть значительные задержки при формировании ответа на запросы либо полный отказ в обслуживании запроса. При подобного рода атаках требования вымогателей всегда связаны с условиями прекращения DDoS-атаки и восстановления работоспособности сетевой инфраструктуры потерпевшего.

Потерпевшей стороной при осуществлении DDoS-атаки являются фирмы, обладающие сетевыми ресурсами, чье взаимодействие с пользователями и потребителями происходит через веб-ресурсы. К ним можно отнести организации: занимающиеся электронной коммерцией, работающие в финансовом секторе, осуществляющие госуслуги, телекоммуникационные услуги, онлайн-обучение, сервисы доставки, социальные сети, мессенджеры, видеоконференции связи. Отметим, что

ввиду особенностей инфраструктуры подобный род атак вымогателей не осуществляется на физических лиц.

Исследование современной литературы в области анализа личности кибер-вымогателей и практики производства судебных компьютерно-технических экспертиз позволяет сделать вывод, что сегодня нельзя говорить о совершении компьютерного преступления, квалифицируемого по ст. 163 УК РФ лицом единолично. Мы имеем дело с повторяющимися, детально подготовленными преступлениями со сложным, многоступенчатым механизмом, основанном на полноструктурном способе преступления, когда сокрытие зачастую происходит одновременно или даже ранее приготовления к преступлению. Такие деяния могут осуществляться только организованными преступными группами, включающими: организатора преступной группы; специалистов в области IT-технологий и программирования; лиц, обладающих компетенциями в области компьютерных технологий и обеспечивающих распространение вредоносных программ, их эксплуатацию с целью последующего перевода кибервалюты в денежные средств и перевод этих средств на подконтрольные счета; лиц, осуществляющие снятие наличных денежных средств со счетов или в банкоматах.

В заключении отметим, что указанные способы, особенно совершаемые организованными преступными группами, могут быть применены для совершения целого ряда иных компьютерных преступлений. «кибершантаж» выбран для примера и в силу его распространённости. Таким образом, информационно-компьютерные криминалистические модели компьютерных преступлений могут служить основой при построении частных криминалистических преодоления противодействию расследования компьютерных преступлений.

Заключение

По итогам анализа судебной практики по делам, связанным с совершением киберпреступлений, можно сделать следующие основные выводы:

1. Под киберпреступностью следует понимать социально-правовое, исторически изменчивое, негативное, массовое явление, представляющее собой совокупность киберпреступлений, совершенных лицами на определенной территории в определенный период времени, обладающее количественными и качественными показателями. Однако на законодательном уровне в России понятия киберпреступления не закреплено, что порождает трудность в установлении указанной выше совокупности и обуславливает необходимость установления перечня составов преступлений, подпадающих под киберпреступления.

2. Выделены способы совершения киберзависимых компьютерных преступлений и «традиционных» преступлений с использованием информационно-коммуникационных технологий.

3. Предупреждение преступности традиционно подразделяется на общесоциальное и специальное. Общесоциальное предупреждение киберпреступности должно осуществляться через систему мероприятий, которые смогли бы обеспечить устойчивое и прогрессивное развитие экономической, политической, духовной, социальной сфер жизни общества.

Для настоящего обзора наибольший интерес представляет разработка мер специального предупреждения киберпреступности, к которым можно отнести следующие некоторые меры:

- совершенствование правового регулирования киберпреступлений и киберпреступности. Во-первых, как уже отмечалось в обзоре, на законодательном уровне указанные выше понятия не регламентируются, что порождает трудности не просто в разработке мер по предупреждению киберпреступности, а в первую очередь в понимании таковой. Во-вторых, постепенно складывается практика, в соответствии с которой судами

кассационных инстанций криптовалюта признается предметом хищения. Представляется, что в Постановления Пленума от 30 ноября 2017 года № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», Постановление Пленума Верховного Суда РФ от 27 декабря 2002 года № 29 «О судебной практике по делам о краже, грабеже и разбое» необходимо внести изменения и признать криптовалюту/цифровую валюту предметом хищения.

Более того, на данный момент в законодательстве РФ закреплен еще один относительно новый цифровой объект – цифровые права, к которым относятся цифровые финансовые активы и утилитарные цифровые права. В случае признания криптовалюты предметом хищения, цифровые права также должны быть признаны в качестве предмета преступного посягательства в силу некой схожей правовой природы с цифровой валютой;

- повышение уровня профессионализма субъектов профилактики, в связи с чем необходима подготовка и переквалификация сотрудников правоохранительных органов в сфере информационных технологий; разработка и совершенствование соответствующих методик обучения;

- повышение уровня правовой грамотности населения в сфере информационных технологий и др.

4. Формируется новый подход к квалификации оплаты чужой картой своих покупок. Данное действие не может расцениваться в качестве мошенничества, так как, оплачивая покупки чужой картой, злоумышленник не обманывает продавца, поскольку у сотрудников торговых точек нет обязанности идентификации держателя карты по документам, удостоверяющим его личность. С учетом изложенного, описанные выше действия могут быть квалифицированы по п. «г» ч. 3 ст. 158 УК РФ;

5. Выявлено достаточно большое количество судебных актов, в соответствии с которыми лицу инкриминируется 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), что коррелируется с приведенными в настоящем исследовании статистическими данными.

6. Важно отметить, что квалификация действий по производству наркотического средства по признаку с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет») является необоснованной и подлежит исключению из приговора, поскольку указанный квалифицирующий признак предусмотрен лишь применительно к сбыту наркотических средств, психотропных веществ или их аналогов;

7. Размещенная ссылка на видеофайл порнографического характера на своей странице в социальной сети может свидетельствовать о наличии умысла на незаконный оборот порнографических материалов, поскольку другие пользователи сети «Интернет» имеют возможность просматривать содержание указанного видеофайла;