Министерство внутренних дел Российской Федерации
Барнаульский юридический институт МВД России

ОСОБЕННОСТИ КВАЛИФИКАЦИИ И ПРЕДУПРЕЖДЕНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Учебное пособие

Барнаул
2024

УДК 343.85:004.738.2(075.8)
ББК 67.408.135я73
О 754

Авторский коллектив:

Ботвин И. В., канд. юрид. наук, доцент — 2.2 (совместно с Ермаковой О. В.); **Ермакова О. В.,** канд. юрид. наук, доцент — 2.2 (совместно с Ботвиным И. В.), 2.3 (совместно с Малетиной М. А., Шагановой О. М.), 2.4 (совместно с Шагановой О. М.), **Малетина М. А.,** канд. юрид. наук — глава 1, 2.1 (совместно с Шагановой О. М.), 2.3 (совместно с Ермаковой О. В., Шагановой О. М.); **Шаганова О. М.,** канд. юрид. наук — 2.1 (совместно с Малетиной М. А.), 2.3 (совместно с Ермаковой О. В., Малетиной М. А.), 2.4 (совместно с Ермаковой О. В.).

Рецензенты:

Ивушкина О. В. — начальник кафедры уголовного права и криминологии Восточно-Сибирского института МВД России, кандидат юридических наук, доцент;

Юшина Ю. В. — старший преподаватель кафедры уголовного права и криминологии Крымского филиала Краснодарского университета МВД России, кандидат исторических наук.

О 754 Особенности квалификации и предупреждения преступлений, совершаемых с использованием информационно-телекоммуникационных технологий : учебное пособие / И. В. Ботвин, О. В. Ермакова, О. М. Шаганова, М. А. Малетина. — Барнаул : Барнаульский юридический институт МВД России, 2024. — 100 с.
ISBN 978-5-94552-585-6

В учебном пособии представлены криминологическая характеристика преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, а также особенности уголовно-правового предупреждения указанных деяний. Авторами систематизированы проблемы толкования признаков преступлений против личности, собственности, компьютерной информации, здоровья населения и общественной нравственности, совершаемых в IT-сфере, предложены алгоритмы квалификации, позволяющие обеспечить реализацию уголовной ответственности.

Учебное пособие предназначено для сотрудников органов внутренних дел, а также преподавателей, курсантов, студентов и слушателей высших учебных заведений и всех интересующихся проблемами уголовного права.

УДК 343.85:004.738.2(075.8)
ББК 67.408.135я73

ISBN 978-5-94552-585-6

ВВЕДЕНИЕ

Обеспечение безопасности в сфере информационно-телекоммуникационной среды на сегодняшний день приобретает первостепенное значение для государственных органов Российской Федерации. Данное положение обусловлено тотальным увеличением количества преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, что отмечается на совещаниях федеральных и ведомственных уровней, в средствах массовой информации и научных сообществах.

Так, на расширенном заседании коллегии МВД России 2024 г. В. В. Путин отметил: «Почти на 30 процентов выросло число преступлений с использованием информационных технологий. Их совершено порядка 680 тысяч, а ущерб превысил 156 миллиардов рублей. Нужно серьёзно совершенствовать механизмы борьбы с правонарушениями в этой сфере…»[1].

В. А. Колокольцев на Правительственной комиссии по профилактике правонарушений в 2023 г. подчеркнул, что за последние пять лет количество противоправных деяний, совершенных с помощью информационных технологий, возросло в два раза и сейчас составляет треть от всех зарегистрированных преступлений[2].

Кроме того, Э. Л. Сидоренко обозначила, что наряду с количественным ростом цифровой преступности наблюдается повышение ее общественной опасности и вредоносности. Если ранее доля тяжких и особо тяжких преступлений в цифровой сфере не превышала 25 %, то в настоящее время она составляет более половины всех цифровых преступлений…[3]

---

[1] Расширенное заседание Коллегии МВД России. 2 апреля 2024 года. URL: http://www.kremlin.ru/events/president/news/73770 (дата обращения: 25.04.2024).

[2] Владимир Колокольцев провел заседание Правительственной комиссии по профилактике правонарушений. URL: https://мвд.рф/news/item/45260331/?year=2024&month= 1&day=1 (дата обращения: 25.04.2024).

[3] Цифровая преступность: угрозы и тренды. Топ-10. URL: https://www.president-sovet.ru/members/blogs/post/tsifrovaya_prestupnost_ugrozy_i_trendy_top_10/ (дата обращения: 25.04.2024).

Появление новых видов преступных форм поведения и механизмов их совершения вносит определенные сложности в деятельность органов дознания, следствия и суда, соответственно, требуются изменения в подходах к квалификации таких деяний, в разработке критериев отграничения от смежных составов преступлений и понятийного аппарата. Эти обстоятельства позволяют говорить об актуальности проблематики, к которой обратились исследователи.

В данной работе будет представлена криминологическая характеристика преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, которая позволит создать картину современного состояния исследуемой категории преступлений, а также выявить общие тенденции и закономерности их развития.

Кроме того, авторами исследуется уголовно-правовое предупреждение преступлений, в которых сеть Интернет выступает либо средством совершения преступления, либо способом: деяния, инспирирующие суицидальное поведение (п. «д» ч. 2 ст. 110, п. «д» ч. 3 ст. 110^1 и ч. 2 ст. 110^2 УК РФ); клевета (ч. 2 ст. 128^1 УК РФ); кража с банковского счета, а равно в отношении электронных денежных средств (п. «г» ч. 3 ст. 158 УК РФ); мошенничество с использованием электронных средств платежа (ст. 159^3 УК РФ); мошенничество в сфере компьютерной информации (ст. 159^6 УК РФ); преступления в сфере компьютерной информации (ст. 272, 273, 274); незаконный сбыт наркотических средств, психотропных веществ или их аналогов, наркосодержащих растений или их частей (п. «б» ч. 2 ст. 228^1 УК РФ); незаконный оборот порнографических материалов или предметов (п. «б» ч. 3 ст. 242, п. «г» ч. 2 ст. 242^1 УК РФ).

Глава 1. Криминологическая характеристика преступности в сфере информационно-телекоммуникационных технологий

Криминологическая обстановка, сложившаяся в стране, требует существенной переориентации деятельности правоохранительных органов на реальное обеспечение криминологической безопасности личности, общества и государства в условиях развития цифровизации общества.

Проблема противодействия цифровой преступности в настоящее время приобретает особую актуальность, поскольку внедрение во все сферы жизнедеятельности цифровых технологий осуществляется быстрыми темпами, что не позволяет в должной степени подготовить механизмы по снижению уровня угроз безопасности. Анализ современного состояния отдельных преступлений против личности, в сфере незаконного оборота наркотических средств, преступлений в сфере экономики, совершенных с использованием информационно-телекоммуникационных технологий, а также преступлений в сфере компьютерной информации показывает, что на протяжении последних лет они имеют устойчивую тенденцию к росту.

Изменение структуры преступности связано, прежде всего, с переориентацией в 2020 г. всей государственной системы безопасности на противодействие эпидемиологической угрозе и введением ограничительных мер, направленных на поддержку населения во время пандемии. Кредитные каникулы, дополнительные выплаты семьям, имеющим детей, снижение ставок по ипотечным кредитам не решили финансовые трудности, возникшие вследствие перевода значительной части населения на удаленную работу. Замкнутость в собственном жилье, оторванность от общения, ограниченная возможность зарабатывания денежных средств, а также активное развитие информационно-телекоммуникационных технологий привели к существенному

увеличению количества преступлений, совершенных с их использованием (см. таблицу 1).

Таблица 1

Количество зарегистрированных преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации

		2019 г.	2020 г.	2021 г.	2022 г.	2023 г.
Всего зарегистрировано преступлений		294 409	510 396	517 772	522 065	676 951
Совершенных с использованием или применением	**расчетных (пластиковых) карт**	34 383	190 167	165 658	127 149	132 849
	компьютерной техники	18 261	28 653	27 519	29 140	36 385
	программ грамм-ных средств	6283	10 050	7216	7649	12 175
	фиктивных элек-элек-тронных платежей	984	1374	954	1325	1608
	сети Интернет	157 036	300 337	351 463	381 112	526 794
	средств мобильной связи	116 154	218 739	217 552	212 963	302 865

Так, в 2020 г. зарегистрировано на 73,4 % больше преступлений, совершенных с использованием информационно-телекоммуникационных технологий, чем в предшествующем 2019 г. Их общее количество составило 510 396. В общем числе зарегистрированных преступлений их удельный вес увеличился с 14,5 % до 25,0 %. При этом следует отметить, что основная масса таких преступлений совершена с использованием или

применением сети Интернет (300 337, +91,3 %), средств мобильной связи (218 739, +88,3 %), а также расчетных (пластиковых) карт (190 167, +453,1 %). Несколько реже при совершении рассматриваемых посягательств в 2020 г. использовались или применялись компьютерная техника (28 653, +56,9 %), программные средства (10 050, +60,0 %), фиктивные электронные платежи (1 374, +39,6 %)[1].

В 2021 г. продолжает наблюдаться рост общего числа зарегистрированных преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, в сравнении с 2020 г. их количество увеличилось на 1,4 % и составило 517 772. В общем числе зарегистрированных преступлений их удельный вес увеличился с 25,0 % до 25,8 %. По-прежнему основная часть подобных преступлений совершается с использованием сети Интернет, их количество из числа зарегистрированных преступлений составило 351 463, что на 17 % больше, чем за аналогичный период прошлого года. Вместе с тем наблюдается снижение количества зарегистрированных преступлений, совершенных с использованием или применением средств мобильной связи (217 552, -0,5 %), расчетных (пластиковых) карт (165 658, -12,9 %), компьютерной техники (27 519, -4,0 %), программных средств (7 216, -28,2 %), фиктивных электронных платежей (954, -30,6 %)[2].

За 2022 г. рост рассматриваемых посягательств также продолжает увеличиваться, количество зарегистрированных преступлений, совершенных с использованием информационно-телекоммуни-кационных технологий или в сфере компьютерной информации, составило 522 065 (+0,8 % по сравнению с аналогичным периодом прошлого года). В общем числе зарегистрированных преступлений их удельный вес увеличился с 25,8 % до 26,5 %. При этом следует отметить, что на 8,4 % увеличилось

[1] Состояние преступности в России за 2020 г. // Министерство внутренних дел Российской Федерации: официальный сайт. URL: https://xn--b1aew.xn--p1ai/dejatelnost/statistics (дата обращения: 08.05.2024).

[2] Состояние преступности в России за 2021 г. // Министерство внутренних дел Российской Федерации: официальный сайт. URL: https://xn--b1aew.xn--p1ai/dejatelnost/statistics (дата обращения: 08.05.2024).

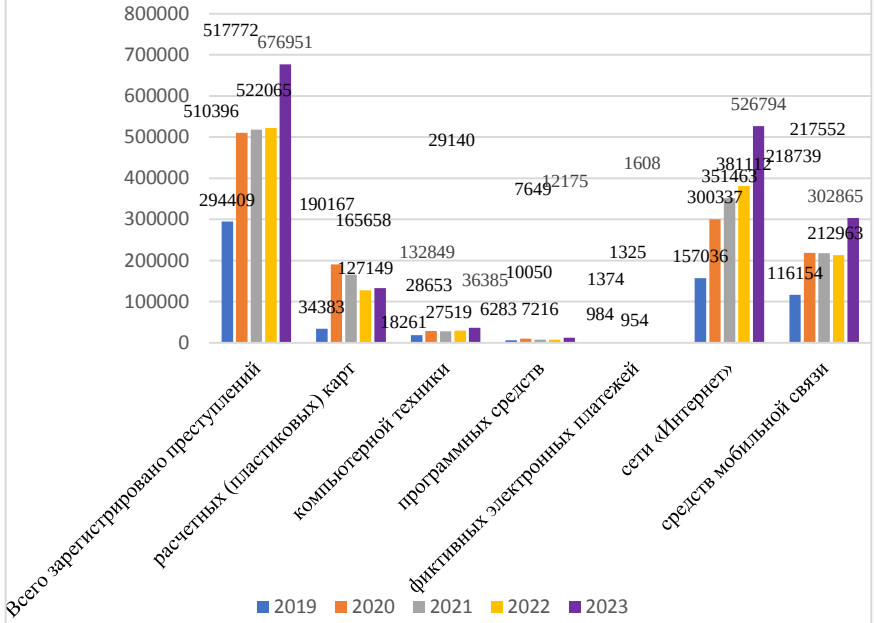
число противоправных деяний, совершенных с использованием или применением сети Интернет (381 112); на 5,9 % — с использованием компьютерной техники (29 140), на 6 % — с применением программных средств (7649); на 38,9 % — с использованием фиктивных электронных платежей (1325). Одновременно на 2,1 % сократилось количество преступлений, совершенных с применением средств мобильной связи (212 963) и на 23,2 % — с использованием расчетных (пластиковых) карт (127 149)[1].

За истекший 2023 г. количество зарегистрированных преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, увеличилось на 29,7 % и составило уже 676 951 преступление. В общем числе зарегистрированных преступлений их удельный вес увеличился с 26,5 % в январе — декабре 2022 г. до 34,8 %. Основную часть рассматриваемых противоправных посягательств составляют преступления, совершенные с использованием сети Интернет, в сравнении с предшествующим годом их количество увеличилось на 38,2 % и составило 526 794. Также продолжает увеличиваться количество преступлений, совершенных с использованием или применением: средств мобильной связи (302 865, +42,2 %); расчетных (пластиковых) карт (132 849, +4,5 %); компьютерной техники (36385, +24,9 %); программных средств (12 175, +59,2 %); а также фиктивных электронных платежей (1 608, +21,4 %) (см. диаграмму 1)[2].

[1] Состояние преступности в России за 2022 г. // Министерство внутренних дел Российской Федерации: официальный сайт. URL: https://xn--b1aew.xn--p1ai/dejatelnost/statistics (дата обращения: 08.05.2024).

[2] Там же.

Диаграмма 1. Количество зарегистрированных преступлений в сфере цифровых технологий, совершенных с использованием расчетных (пластиковых) карт, компьютерной техники, программных средств, фиктивных электронных платежей, сети Интернет, средств мобильной связи



Сравнительный анализ данных по годам, представленных на диаграмме 1, показывает, что на протяжении последних четырех лет при совершении преступного деяния чаще всего используется сеть Интернет (58,8 % в 2020 г., 67,9 % в 2021 г., 73,0 % в 2022 г. и 77,8 % в 2023 г.). Кроме того, наблюдается устойчивая тенденция к росту числа зарегистрированных преступлений, совершенных с ее использованием.

Относительно количества преступлений, совершенных при помощи средств мобильной связи, следует отметить, что в 2020 г. в регистрации произошел их резкий скачок (на 88,3 %). Несмотря на некоторое снижение их числа в 2021–2022 гг. (на

0,5 % и 2,1 % соответственно), необходимо подчеркнуть, что преступники при совершении цифровых преступлений отдают предпочтение мобильной связи (42,9 % в 2020 г., 42,0 % в 2021 г., 40,8 % в 2022 г. и 44,7 % в 2023 г.).

Третье место в количестве зарегистрированных преступлений занимают деяния, совершенные с применением расчетных (пластиковых карт). В 2020 г. их число возросло на 453,1 %, однако в последующие годы наблюдается некоторое снижение — на 12,9 % в 2021 г. и 23,2 % в 2022 г. В 2023 г. их количество снова немного увеличилось — на 4,5 %.

Существующее в настоящее время разнообразие преступных проявлений, совершаемых в цифровой среде, не позволяет исчерпывающим образом рассмотреть их современное состояние. Ввиду отсутствия официальной статистической отчетности о преступлениях против личности, совершаемых с использованием информационно-телекоммуникационных технологий, анализу подвергнуты отдельные преступления против собственности, здоровья населения и общественной нравственности, а также в сфере компьютерной информации (см. таблицу 2).

Таблица 2

Количество отдельных зарегистрированных преступлений, совершенных с использованием информационно-телекоммуникационных технологий, в период 2019–2023 гг.

Статьи УК РФ	2019 г.	2020 г.	2021 г.	2022 г.	2023 г.
п. «г» ч. 3 ст. 158 удельный вес	**98 798** 4,9 %	**173 416** 8,5 %	**156 792** 7,8 %	**113 565** 5,8 %	**119 212** 6,1 %
ст. 159 удельный вес	**119 903** 5,9 %	**210 493** 10,3 %	**238 560** 11,9 %	**249 984** 12,7 %	**353 201** 18,1 %
ст. 159^{3} удельный вес	**16 119** 0,8 %	**25 820** 1,3 %	**10 258** 0,5 %	**7 288** 0,4 %	**2 461** 0,1 %
ст. 159^{6} удельный вес	**687** 0,03 %	**761** 0,04 %	**431** 0,02 %	**334** 0,02 %	**417** 0,02 %

Статьи УК РФ	2019 г.	2020 г.	2021 г.	2022 г.	2023 г.
ст. 242–242[2] удельный вес	**1 916** 0,09 %	**2099** 0,1 %	**2299** 0,11 %	**2588** 0,13 %	**3 121** 0,16 %
ст. 272 удельный вес	**2 420** 0,12 %	**4 105** 0,2 %	**6 392** 0,3 %	**9 308** 0,5 %	**36 788** 1,8 %
ст. 273 удельный вес	**455** 0,02 %	**371** 0,02 %	**317** 0,02 %	**200** 0,01 %	**196** 0,01 %
ст. 274 удельный вес	0	0	1	0	0
п. «б» ч.2 ст. 228[1] удельный вес	**24 677** 1,2 %	**47 060** 2,3 %	**51 444** 2,6 %	**62 209** 3,2 %	**81 520** 4,2 %

Анализ статистических данных по отдельным видам преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, показывает, что в условиях пандемии произошел огромный скачок совершения преступлений против собственности. К примеру, в 2020 г. количество зарегистрированных краж с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного ст. 159[3] УК РФ) возросло на 75,5 %. Удельный вес данных преступлений в общей структуре преступности вырос с 4,9 % до 8,5 %. На 75,6 % увеличилось количество зарегистрированных мошенничеств. Их удельный вес в рассматриваемый период составил 10,3 %, что практически в два раза превышает рассматриваемый показатель за аналогичный период предыдущего года. Кроме того, с 16 119 до 25 820, или на 60,2 %, увеличилось количество зарегистрированных мошенничеств с использованием электронных средств платежа. Незначительно (на 10,8 %) увеличилось количество зарегистрированных мошенни-

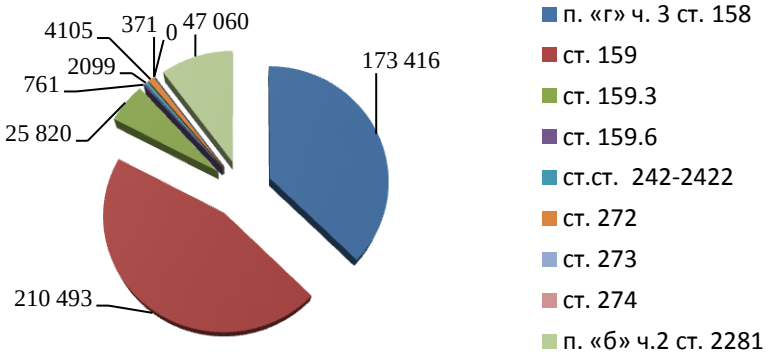
честв в сфере компьютерной информации. Их удельный вес в общей структуре преступности в период пандемии остался примерно на том же уровне.

Активное использование населением в условиях ограничительных мер современных цифровых средств создало благоприятную почву и для совершения преступлений против здоровья населения и общественной нравственности. Так, на 90,7 % увеличилось количество зарегистрированных незаконных производства, сбыта или пересылки наркотических средств, психотропных веществ или их аналогов, а также незаконных сбыта или пересылки растений, содержащих наркотические средства или психотропные вещества, либо частей, содержащих наркотические средства или психотропные вещества. Удельный вес рассматриваемых посягательств в общей структуре преступности увеличился практически в два раза (с 1,2 % до 2,3 %). Также на 9,6 % возросло число зарегистрированных преступлений, предусмотренных ст. 242–242[2] УК РФ (изготовление порнографических материалов).

Относительно преступлений в сфере компьютерной информации следует отметить, что на 69,6 % увеличилось количество зарегистрированных неправомерных доступов к компьютерной информации, но на 18,5 % сократилось количество зарегистрированных фактов создания, использования и распространения компьютерных программ[1] (см. диаграмму 2).

[1] Состояние преступности в России за 2020 г. // Министерство внутренних дел Российской Федерации: официальный сайт. URL: https://xn--b1aew.xn--p1ai/dejatelnost/statistics (дата обращения: 08.05.2024).

Диаграмма 2. Количество отдельных зарегистрированных преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, в 2020 г.



В последующие годы происходит постепенное снижение количества зарегистрированных краж с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного ст. 159[3] УК РФ). В 2021 г. их число составило 156 792 (-9,6 %), в 2022 г. — 113 565 (-27,6 %). Удельный вес рассматриваемых посягательств в общей структуре преступности составляет 7,8 % и 5,8 % в 2021 г. и 2022 г. соответственно. Кроме того, происходит снижение в регистрации мошенничеств с использованием электронных средств платежа — на 60,3 % в 2021 г. и 29,0 % в 2022 г., а также мошенничеств в сфере компьютерной информации — на 43,4 % в 2021 г. и 22,5 % в 2022 г.

Вместе с тем в целом количество мошеннических действий, совершенных с использованием информационно-телекоммуникационных технологий, продолжает увеличиваться. В 2021 г. их количество составило 238 560 (+13,3 %), в 2022 г. — 249 984 (+4,8 %). Удельный вес данных преступлений в общей структуре преступности также увеличился и составил 11,9 % и 12,7 % соответственно.

Также происходит увеличение количества зарегистрированных преступлений против здоровья населения и общественной нравственности. В 2021 г. число преступлений, предусмотренных ст. 242–242[2] УК РФ (изготовление порнографических материалов), выросло на 9,5 %, в 2022 г. — на 12,6 %. Число зарегистрированных незаконных производства, сбыта или пересылки наркотических средств, психотропных веществ или их аналогов, а также незаконных сбыта или пересылки растений, содержащих наркотические средства или психотропные вещества, либо частей, содержащих наркотические средства или психотропные вещества, в 2021 г. составило 51 444 (+9,3 %), в 2022 г. — 62 209 (+20,9 %). Их удельный вес также увеличился и составил 2,6 % в 2021 г. и 3,2 % в 2022 г.

Результаты исследования преступлений в сфере компьютерной информации свидетельствуют о росте количества зарегистрированных преступлений, предусмотренных ст. 272 УК РФ (неправомерный доступ к компьютерной информации). В 2021 г. их общее количество составило 6392 (+55,7 %), в 2022 г. — уже 9308 (+45,6 %). Удельный вес данных преступных посягательств в общей структуре преступности увеличился до 0,3 % в 2021 г. и до 0,5 % в 2022 г. Вместе с тем снижается количество зарегистрированных преступлений, предусмотренных ст. 273 УК РФ (создание, использование и распространение вредоносных компьютерных программ) — до 317 (-14,6 %) в 2021 г. и до 200 (-36,9 %) в 2022 г.[1] (см. диаграммы 3, 4).

[1] Состояние преступности в России за 2021–2022 гг. // Министерство внутренних дел Российской Федерации: официальный сайт. URL: https://xn--b1aew.xn--p1ai/dejatelnost/statistics (дата обращения: 08.05.2024).

Диаграмма 3. Количество отдельных зарегистрированных преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, в 2021 г.

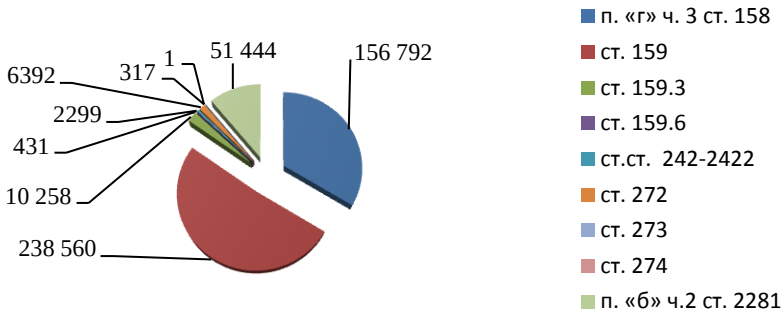
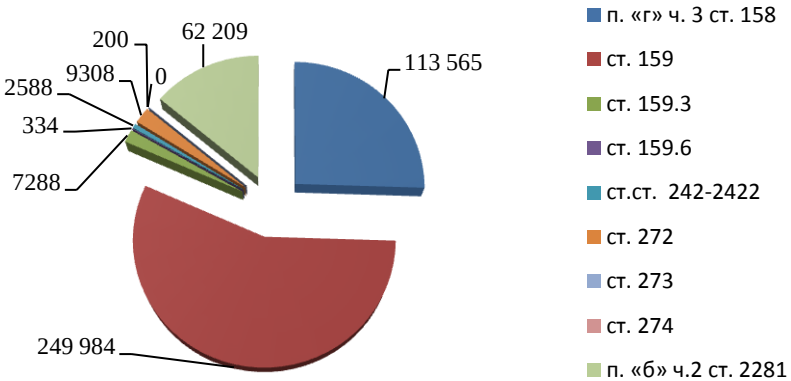


Диаграмма 4. Количество отдельных зарегистрированных преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере комьютерной информации, в 2022 г.



В 2023 г. на 5 % произошло увеличение количества зарегистрированных краж с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного ст. 159[3] УК РФ). В истекшем

2023 году их число равно 119 212 (+5 %), удельный вес рассматриваемых посягательств в общей структуре преступности составил 6,1 %. Вместе с тем на 66,2 % произошло снижение в регистрации мошенничеств с использованием электронных средств платежа.

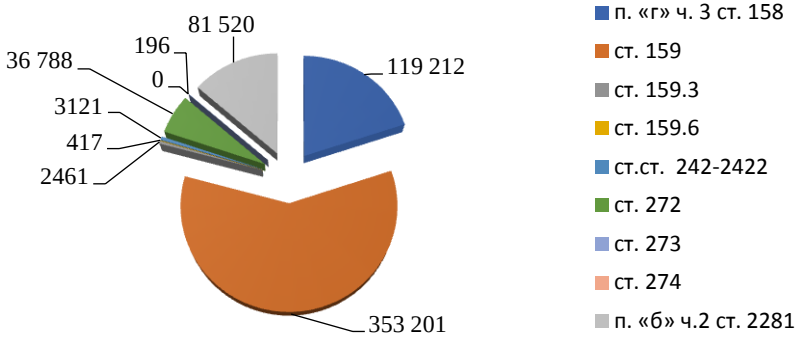
В целом количество мошеннических действий, совершенных с использованием информационно-телекоммуникационных технологий, продолжает увеличиваться. В истекшем 2023 году их количество составило 353 201 (+41,3 %), удельный вес данных преступлений в общей структуре преступности также увеличился и составил 18,1 %.

Происходит и рост количества зарегистрированных преступлений против здоровья населения и общественной нравственности. В 2023 г. число преступлений, предусмотренных ст. 242–242^2 УК РФ (изготовление порнографических материалов), увеличилось на 20,8 % и составило 3127 преступлений. Число зарегистрированных незаконных производства, сбыта или пересылки наркотических средств, психотропных веществ или их аналогов, а также незаконных сбыта или пересылки растений, содержащих наркотические средства или психотропные вещества, либо частей, содержащих наркотические средства или психотропные вещества, в 2023 г. составило 81 520 (+31 %), их удельный вес также увеличился и соответствовал 4,2 %.

Результаты исследования преступлений в сфере компьютерной информации свидетельствуют о значительном росте (+295,2 %) количества зарегистрированных преступлений, предусмотренных ст. 272 УК РФ (неправомерный доступ к компьютерной информации). В истекшем 2023 году их общее количество составило 36 788, удельный вес данных преступных посягательств в общей структуре преступности увеличился до 1,8 %. Вместе с тем снижается количество зарегистрированных преступлений, предусмотренных ст. 273 УК РФ (создание, использование и распространение вредоносных компьютерных программ), — до 196 (-2 %)[1] (см. диаграмму 5).

[1] Состояние преступности в России за 2023 гг. // Министерство внутренних дел Российской Федерации: официальный сайт. URL: https://xn--b1aew.xn--p1ai/dejatelnost/statistics (дата обращения: 08.05.2024).

Диаграмма 5. Количество отдельных зарегистрированных преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, в 2023 г.



В рамках анализа состояния цифровой преступности представляется необходимым остановиться и на раскрываемости данного блока преступлений. Высокий рост в 2020 г. количества рассматриваемых преступных посягательств при отсутствии специальной подготовки правоохранительных органов в сфере цифровых технологий, законодательной базы и методических рекомендаций по проблемным вопросам квалификации преступлений, совершаемых с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, привел к снижению процента их раскрываемости (в 2019 г. процент раскрываемости составлял 24 %, в 2020 г. он снизился до 20 %). Несмотря на некоторое увеличение рассматриваемого показателя в 2021–2022 гг., который составил уже 23,4 % и 27,8 % соответственно, общее количество нераскрытых цифровых преступлений оставалось высоким (388 607 преступлений в 2021 г. и 370 179 преступлений в 2022 г.). В истекшем 2023 г. количество нераскрытых преступлений, совершенных с использованием информационно-телекоммуникационных тех-

нологий или в сфере компьютерной информации, составило 172 290, процент раскрываемости снизился до 26,6 %[1].

Подводя итог рассмотрению состояния преступлений, совершаемых с использованием современных цифровых средств, следует признать, что, несмотря на незначительные колебания, динамика данного вида преступности характеризуется тенденцией к постоянному росту, увеличением числа преступлений, совершенных посредством использования сети Интернет. Указанные обстоятельства требуют от государства выработки принципиально новых подходов для борьбы с данным явлением.

[1] Состояние преступности в России за 2019-2023 гг. // Министерство внутренних дел Российской Федерации: официальный сайт. URL: https://xn--b1aew.xn--p1ai/dejatelnost/statistics (дата обращения: 08.05.2024).

Глава 2. Предупреждение преступности в сфере информационно-телекоммуникационных технологий уголовно-правовыми средствами

2.1. Уголовно-правовое предупреждение преступлений против личности, совершаемых с использованием информационно-телекоммуникационных технологий

В настоящее время информационно-телекоммуникационная сеть Интернет используется при совершении преступлений не только в сфере экономики, против общественной безопасности и общественного порядка, но и против личности. В частности, рассматриваемый признак характерен для комплекса уголовно-правовых норм, призванных осуществлять охрану жизни человека от посягательств, обозначаемых в научной литературе как *преступная причастность к самоубийству*.

С учетом относительно непродолжительного времени, прошедшего с момента криминализации норм об ответственности за склонение к совершению самоубийства или содействие его совершению (ст. 110^1 УК РФ), организацию деятельности, направленной на побуждение к совершению самоубийства (ст. 110^2 УК РФ), расширения рамок состава преступления, предусматривающего ответственность за доведение до самоубийства (ст. 110 УК РФ), а также отсутствия разъяснений высшего судебного органа России, которые бы содержали правила толкования данных составов, в следственно-судебной практике нередко возникают спорные вопросы при квалификации указанных деяний.

Дифференциация ответственности за совершение рассматриваемых преступных посягательств посредством использования информационно-телекоммуникационной сети Интернет является вполне обоснованным и перспективным законодательным решением ввиду того, что эти посягательства обладают повышенной

степенью общественной опасности, продиктованной глобальным характером, определенной степенью анонимности пользователей, преодолением географической разобщенности, подростковой аудиторией, эффективностью достижения преступного результата и минимальной вероятностью привлечения виновного к уголовной ответственности[1].

Вместе с тем рассматриваемый квалифицирующий признак доведения до самоубийства, склонения к совершению самоубийства или содействия его совершению, организации деятельности, направленной на побуждение к совершению самоубийства, не указывает на наличие самостоятельного состава и должен сопровождаться основными признаками объективной стороны одного из преступлений, предусмотренных ст. 110, 110^1 или 110^2 УК РФ.

В целях разграничения составов преступлений, регламентированных п. «д» ч. 2 ст. 110, п. «д» ч. 3 ст. 110^1 и ч. 2 ст. 110^2 УК РФ, считаем необходимым подробно остановиться на признаках их объективной стороны.

Следует отметить, что рассматриваемые преступные посягательства совершаются с использованием информационно-телекоммуникационных технологий, под которыми, согласно ст. 2 Федерального закона Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», понимаются технологические системы, предназначенные для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники[2], т. е. удаленно, без непосредственного контакта виновного с потерпевшим. Самой общедоступной из таких систем является глобальная децентрализованная информационно-телекоммуникационная сеть Интернет.

---

[1] Филиппова С. В. Склонение к совершению самоубийства или содействие совершению самоубийства: уголовно-правовая характеристика и проблемы квалификации: дис. … канд. юрид. наук. М., 2020. С. 121.

[2] Об информации, информационных технологиях и о защите информации [Электронный ресурс]: федеральный закон Российской Федерации от 27.07.2006 № 149-ФЗ (ред. от 12.12.2023). Доступ из справ.-правовой системы «КонсультантПлюс».

Совершение преступлений, инспирирующих суицид, посредством использования информационно-телекоммуникационной сети Интернет в целом представляет собой размещение в социальных сетях или мессенджерах сообщений и информационных материалов, побуждающих к совершению самоубийства.

Следует отметить, что бесконтактный способ доведения до самоубийства исключает возможность непосредственного физического воздействия на потерпевшего. В связи с этим объективная сторона преступления, предусмотренного п. «д» ч. 2 ст. 110 УК РФ, выражается в размещении в социальных сетях, мессенджерах, форумах и на сайтах сети Интернет всевозможных текстовых и видеосообщений, содержащих угрозы и оскорбления в адрес конкретного лица, циничные насмешки; фотографий с компрометирующими сведениями, а также сведениями, унижающими его человеческое достоинство, имеющих своей целью довести потерпевшего до самоубийства. Совокупность же упомянутых действий может указывать на признак жестокого обращения с потерпевшим, выражающегося в дестабилизации его эмоционального состояния[1].

Наиболее распространенной в настоящее время формой доведения до самоубийства с использованием сети Интернет является кибербуллинг — запугивание и травля с использованием социальных сетей, приложений для обмена сообщениями, игровых платформ, мобильных телефонов.

В России первый приговор по п. «д» ч. 2 ст. 110 УК РФ был вынесен в Краснодарском крае в отношении С., которая отомстила бросившему ее парню, вернувшемуся из армии. Под вымышленными именами она зарегистрировалась на сайте популярной социальной сети и рассылала знакомым В. Г. сообщения, содержащие не соответствующие действительности сведения о его нетрадиционной сексуальной ориентации. На его личной странице в сети Интернет она систематически оставляла записи, унижающие

[1] Ханова И. В. Использование IT-технологий при совершении преступлений против жизни, связанных с суицидом: уголовно-правовой аспект // Вестник Волгоградской академии МВД России. 2022. № 2 (61). С. 74.

его достоинство. В результате под армейскими фотографиями молодого человека начали появляться критические комментарии. Будучи убежденным, что его честь опорочена, В. Г. не выдержал травли и совершил самоубийство путем повешения[1].

Еще одной формой доведения до самоубийства с использованием информационно-телекоммуникационной сети Интернет являются действия кураторов так называемых «групп смерти» в отношении участников суицидальных игр, которые отказываются от выполнения последнего задания.

Например, в ходе проведения предварительного расследования уголовного дела по обвинению жителя г. Москвы С. по п. «д» ч. 2 ст. 110 УК РФ было установлено, что, являясь куратором группы «Синий кит», в которую входили 32 ребенка, он давал им задания, направленные на причинение вреда своему здоровью, склонение их к самоубийству. Количество заданий было от одного до пятидесяти, среди них следующие: сделать длинный порез от сгиба локтя до запястья, вырезать на руке кита, порезать губу, смотреть фильмы ужасов, ни с кем не общаться и т. п. Последним из них было совершение самоубийства. Одной из участников данной группы была четырнадцатилетняя школьница из Челябинской области, которая, испугавшись, отказалась от выполнения задания, заключавшегося в совершении самоубийства путем повешения или прыжка с многоэтажного здания. После этого деяние С., начатое как склонение к самоубийству посредством использования информационно-телекоммуникационной сети Интернет (п. «д» ч. 3 ст. 110[1] УК РФ), стало содержать признаки состава преступления, предусмотренного п. «д» ч. 2 ст. 110 УК РФ (доведение до самоубийства). Требуя доведения игры до логического завершения, С. начал высказы-

[1] Официальный сайт Лазаревского районного суда г. Сочи. URL: http://sochi-lazarevsky.krd.sudrf.ru/ (дата обращения: 08.05.2024).

вать в адрес школьницы угрозы: «Я приеду и помогу тебе! Не убьешь себя, буду по кускам резать твою маму, всю семью, а потом и тебя!» Для убедительности куратор назвал улицу, на которой проживала школьница вместе с родителями. Испугавшись, она попыталась отравиться, приняв валосердин[1].

Склонение к совершению самоубийства или содействие совершению самоубийства преследуют цель достижения единого результата — совершения конкретным лицом самоубийства, однако от доведения до самоубийства данные преступные посягательства отличаются интеллектуальными способами воздействия на потерпевшего.

Под склонением к самоубийству понимаются «действия, направленные на возбуждение у другого лица желания или решимости совершить самоубийство путем применения к нему исключительно ненасильственных способов воздействия. Помимо указанных в тексте закона (уговоры, предложения, подкуп, обман), к ним следует отнести убеждение, просьбу, совет, указание»[2]. Все вышеперечисленные способы не совместимы с применением угроз, жестоким обращением или систематическим унижением человеческого достоинства, что прямо указано законодателем в диспозиции ст. 110^1 УК РФ.

В судебной практике встречается огромное количество примеров склонения к самоубийству путем уговоров и предложений, совершенного с использованием информационно-телекоммуникационной сети Интернет.

Так, в процессе переписки в общедоступной социальной сети «ВКонтакте» Ф. вовлекла Р. в беседу в целях разжигания интереса к вопросам самоубийства. Затем на протяжении достаточно длительного времени она уговари-

[1] Официальный сайт Ленинского районного суда г. Челябинска. URL: http://lench.chel.sudrf.ru/ (дата обращения: 08.05.2024).

[2] Более подробно см.: Малетина М. А. Уголовно-правовая характеристика преступной причастности к самоубийству, не связанной с доведением до него. М.: Юрлитинформ, 2022. С. 71–104.

вала ее сыграть в игру «Синий кит», заключавшуюся в прохождении 50 уровней, последним из которых являлось совершение самоубийства. В связи с тем, что Р. переживала глубокую депрессию из-за расставания со своим молодым человеком, она согласилась на участие в данной игре и выполнила часть заданий[1].

Кроме того, в процессе переписки в информационно-телекоммуникационной сети Интернет Б. предложила несовершеннолетней Л. выполнить 50 заданий суицидальной направленности, последним из которых должно было стать совершение самоубийства. После выполнения ею первого задания, заключавшегося в вырезании лезвием на руке фразы «Я ошибка природы», преступные действия Б. были пресечены отцом потерпевшей[2].

Примеров склонения к самоубийству путем подкупа и обмана в информационно-телекоммуникационной сети Интернет в судебно-следственной практике не встречается.

Думается, что подкуп может выражаться «в освобождении от имущественных обязательств или затрат потерпевшего, в обещании предоставления каких-либо благ или материальной выгоды его близким родственникам, оказания для них каких-либо услуг (устройство на работу, предоставление жилья, решение финансовых проблем). Эти обещания лицу в выполнении в его интересах каких-либо действий ставятся под условие, что он совершит самоубийство»[3].

Обман со стороны виновного, провоцирующий потерпевшего на суицид, в свою очередь, может заключаться в предоставлении заведомо ложных сведений, касающихся его жизни, например наличия у него неизлечимой болезни, презрения со стороны близких, сверстников или коллег и т. п. «Самой уязвимой категорией при совершении склонения к самоубийству указанным

[1] Архив Невского районного суда г. Санкт-Петербурга за 2018 г. Д. № 1-498.

[2] Архив Татарского районного суда Новосибирской области за 2018 г. Д. № 1-46.

[3] Малетина М. А. Уголовно-правовая характеристика преступной причастности к самоубийству, не связанной с доведением до него. М.: Юрлитинформ, 2022. С. 78.

способом являются подростки, поскольку для них характерна легкая внушаемость. В связи с введением их в заблуждение относительно вышеперечисленных обстоятельств достаточно легко становится убедить их в том, что сложившаяся с ними ситуация является безысходной и самоубийство — это единственный выход»[1].

Основная суть содействия совершению самоубийства заключается в оказании помощи потерпевшему в совершении самоубийства, когда он уже принял решение о его совершении. Отличительной особенностью данной формы преступной причастности к самоубийству является то, что перечень способов совершения данного преступления является исчерпывающим — они прямо предусмотрены в диспозиции ч. 2 ст. 110^1 УК РФ. К ним относятся: советы, указания, предоставление информации, средств или орудий совершения самоубийства либо устранение препятствий к его совершению, а также обещания скрыть средства или орудия совершения самоубийства.

Примером содействия самоубийству, совершенного с использованием информационно-телекоммуникационной сети Интернет, являются действия Г., которая в социальной сети «ВКонтакте» вовлекла несовершеннолетнюю Ф. в беседу в целях разжигания у нее интереса к вопросу суицида. На протяжении двух месяцев она систематически высказывала Ф. советы и давала указания на способы и методы совершения суицида. В результате безысходности Ф. предприняла две попытки самоубийства путем принятия таблеток феназепама и вскрытия вены на запястье[2].

Кроме того, приговором Невского районного суда г. Санкт-Петербурга по п. «а», «д» ч. 3 ст. 110^1 УК РФ Ф. осуждена. Она признана виновной в том, что оказывала содействие в совершении самоубийства несовершеннолетней М. советами и указаниями, а также предоставлением

[1] Малетина М. А. Уголовно-правовая характеристика преступной причастности к самоубийству, не связанной с доведением до него. М.: Юрлитинформ, 2022. С. 78.

[2] Архив Судакского городского суда Республики Крым за 2018 г. Д. № 1-25.

информации о способах самоубийства (падение с крыши здания, нанесение себе телесных повреждений, несовместимых с жизнью, и т. д.)[1].

Главной характеристикой склонения к совершению самоубийства или содействия его совершению является то, что в результате их совершения посредством использования информационно-телекоммуникационной сети Интернет создается реальная угроза жизни и здоровью конкретного потерпевшего. При этом фактического причинения вреда объекту посягательства не требуется, достаточно совершения действий, направленных на создание опасности причинения вреда жизни и здоровью. Вышеизложенное позволяет сделать вывод о том, что момент окончания преступления, предусмотренного п. «д» ч. 3 ст. 110^1 УК РФ, связан с совершением виновным самого факта склонения лица к самоубийству или содействия его совершению независимо от того, наступили последствия в виде совершения самого самоубийства или покушения на него или нет.

Следующей формой преступной причастности к самоубийству является организация деятельности, направленной на побуждение к совершению самоубийства путем распространения информации о способах совершения самоубийства или призывов к совершению самоубийства, сопряженная с использованием информационно-телекоммуникационной сети Интернет. Ответственность за совершение данного преступления предусмотрена ч. 2 ст. 110^2 УК РФ.

Целью установления уголовной ответственности за указанную организационную деятельность, согласно пояснительной записке к законопроекту, является «установление дополнительной уголовной ответственности в отношении организаторов такой опасной для граждан деятельности с возможностью привлечения их к ответственности, когда еще отсутствует конкретная жертва преступления, но имеются все признаки склонения к совершению самоубийства. Например, созданы сайты с соответ-

[1] Архив Невского районного суда г. Санкт-Петербурга за 2018 г. Д. № 1-498.

ствующей суицидальной тематикой или игра, предполагающая вовлечение ребенка в суицидальную модель поведения»[1].

Таким образом, главной особенностью, позволяющей отграничивать рассматриваемый состав от деяния, предусмотренного ч. 1 ст. 110[1] УК РФ (конкретизированное склонение), является то, что действия лица, виновного в организации такой деятельности, направлены на склонение к совершению самоубийства не конкретного лица, а неопределенного круга лиц (неперсонифицированное склонение).

Объективная сторона рассматриваемого преступного посягательства имеет крайне сложную конструкцию. Одновременное использование законодателем при ее описании таких понятий, как «распространение информации о способах совершения самоубийства или призывов к совершению самоубийства», «деятельность, направленная на побуждение к совершению самоубийства посредством распространения подобной информации или призывов к совершению самоубийства», «организация указанной деятельности», вызывает затруднения в понимании того, как они соотносятся между собой.

Представляется, что объективная сторона рассматриваемого преступления выражается в активных действиях виновного по созданию условий и обеспечению передачи сведений или призывов, инспирирующих суицид, по каналам информационно-телекоммуникационной сети Интернет и получению этой информации неопределенным количеством лиц.

К сведениям, побуждающим к совершению самоубийства, может относиться следующая информация:

1) о способах совершения самоубийства;

2) средствах и местах для его совершения;

3) совокупности необходимых для самоубийства условий (выбор места, времени, способа, иные подготовительные дей-

[1] О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных механизмов противодействия деятельности, направленной на побуждение детей к суицидальному поведению: пояснительная записка к проекту федерального закона Российской Федерации № 118634-7. URL: https://sozd.duma.gov.ru/bill/118634-7 (дата обращения: 08.05.2024).

ствия, которые необходимо совершить для достижения цели самоубийства).

В свою очередь, к призывам к совершению самоубийства относится информация, отвечающая одному или нескольким из следующих критериев:

1) наличие предложения, просьбы, приказа совершить самоубийство;

2) наличие указания на самоубийство как на способ решения проблемы;

3) выражение положительной оценки либо одобрение совершения самоубийства либо действий, направленных на самоубийство, или намерений реального (воображаемого) собеседника или третьего лица совершить самоубийство, а также призыва, побуждающего совершить самоубийство;

4) информация, содержащая побуждающие к совершению самоубийства аргументы, включающие утверждения (суждения), не содержащие прямого либо явного побуждения, но способные склонить к принятию решения о совершении самоубийства, в т. ч. посредством приведения конкретных примеров, представляющих собой популяризацию четких действий других людей, которые уже совершили самоубийство, и/или утверждения (суждения) о преимуществах, которые получили лица, совершившие самоубийство, в т. ч. представление самоубийства как обыденного явления (приемлемого, логичного и закономерного в современном обществе поступка);

5) выражение осуждения, высмеивания неудавшейся попытки совершить самоубийство, в т. ч. включающее описание отношения, чувств и обсуждения темы лицами, имеющими опыт попытки самоубийства;

6) наличие любого объявления, в т. ч. о знакомстве, в целях совершения самоубийства, в т. ч. группового и/или ассистированного, осуществленного с чьей-либо помощью либо в чьем-то присутствии, либо под чьим-то наблюдением, а также в целях попытки совершения самоубийства;

7) наличие опроса (голосования), теста, рейтинга на предмет выбора самоубийства как способа решения проблемы, равно как

на предмет выбора наиболее безболезненного, надежного, доступного, эстетичного способа самоубийства.

В силу отнесения состава преступления, предусмотренного ч. 2 ст. 110^2 УК РФ, по конструкции объективной стороны к формальному составу преступления для юридической оценки размещения информации суицидального характера или призывов к совершению самоубийства в информационно-телекоммуникационной сети Интернет не имеет значения, какое количество людей ознакомилось с указанной информацией или призывом. Определяющим фактором в данном случае выступает доступность информации для широкого круга лиц.

Так, Абаканским городским судом Республики Хакасия по ч. 2 ст. 110^2 УК РФ к пяти годам шести месяцам лишения свободы с отбыванием наказания в исправительной колонии строгого режима был осужден гражданин А.

В целях побуждения неопределенного круга лиц к самоубийству в мессенджере Telegram он создал публичный канал «Лицо суицида», доступный для просмотра и обмена электронными сообщениями неограниченному кругу лиц — пользователям мессенджера Telegram в сети Интернет, который в дальнейшем использовал для побуждения неограниченного круга лиц (посетителей канала) к самоубийству путем распространения информации о способах совершения самоубийства и призывов к совершению самоубийства в публикуемых на канале электронных сообщениях, содержащих текст, графические и видеоматериалы соответствующей его преступному умыслу тематики. На публичный канал «Лицо суицида», в котором А. разместил в форме электронных сообщений информацию о способах совершения самоубийства и призывы к совершению самоубийства, было подписано 3000 пользователей[1].

[1] Архив Абаканского городского суда Республики Хакасия за 2021 г. Д. № 1-346.

Следующий аспект, на который особо следует обратить внимание, — это разграничение составов преступлений, предусмотренных п. «д» ч. 3 ст. 110^1 и ч. 2 ст. 110^2 УК РФ, друг от друга. В пояснительной записке к проекту Федерального закона Российской Федерации от 7 июня 2017 г. № 120-ФЗ его разработчики, обосновывая общественную опасность криминализированных посягательств, указывают на тот факт, что склонение к совершению самоубийства или содействие его совершению всегда влекут опасные последствия в отношении конкретных лиц, а действия по организации деятельности, направленной на побуждение к совершению самоубийства, представляют собой неконкретизированный характер.

Следует отметить, что ввиду отсутствия каких-либо официальных разъяснений в части квалификации действий виновного, содержащих в себе одновременно персонифицированное воздействие и воздействие в отношении неконкретизированной категории потерпевших, в правоприменительной практике встречаются различные варианты квалификации.

Так, Г., будучи пользователем общедоступной социальной сети «ВКонтакте», достоверно зная о повышенном интересе значительной части пользователей указанной социальной сети к темам самоубийства, депрессии и иного деструктивного контента (информации), систематически размещал на имеющихся в его распоряжении персональных электронных страницах ***общедоступную*** *(выделено авт. — М. М.) информацию суицидального характера, в т. ч. с использованием гиперссылок, объединяющих публичные сообщения определенной тематики, размещенные в информационно-телекоммуникационной сети Интернет (хештег), тем самым завлекал на свои страницы лиц, имеющих намерения совершить суицид, с целью дальнейшего склонения данных лиц к совершению самоубийства. После организации деятельности, направленной на побуждение к совершению самоубийства, он вступил в личную электронную переписку одновременно с несколькими пользователями, проживающими в разных городах России.*

В ходе переписки он разъяснял им правила участия в данной беседе и давал различные задания, формирующие у указанных лиц депрессивную направленность сознания, тем самым снимая у них психологический барьер, препятствующий совершению суицида выбранным ими способом. Четыре человека, состоявшие в этой конференц-беседе, вышли из нее после выполнения нескольких заданий.

В ходе личной переписки с Б. виновный призывал ее покончить жизнь самоубийством путем падения с высотного здания. Кроме того, неоднократно призывал ее к совершению последовательных аутоагрессивных действий: ежедневно резать различные части своего тела, бывать в местах, опасных для жизни, и фотографироваться там, совершать иные действия, имитирующие распространенные способы самоубийства[1].

Анализ описательной части данного приговора позволяет прийти к выводу о том, что, помимо признаков состава преступления, предусмотренного ч. 2 ст. 110^2 УК РФ, в действиях Г. по отношению к Б. содержатся также признаки состава преступления, предусмотренного п. «д» ч. 3 ст. 110^1 УК РФ (склонение к совершению самоубийства путем уговоров и предложений при отсутствии признаков доведения до самоубийства, совершенное в информационно-телекоммуникационной сети Интернет).

Однако в мотивировочной части приговора суд указал, что *действия подсудимого органами предварительного следствия ошибочно квалифицированы как два преступления (первое в отношении неопределенного круга лиц, второе — в отношении Б.). Из предъявленного обвинения и установления обстоятельств дела в судебном заседании установлено, что подсудимый, реализуя свой преступный умысел, по обоим преступлениям для посещения общедоступной социальной сети «ВКонтакте» каждый раз использовал один и тот же мобильный телефон, одни и те*

[1] Архив Люберецкого городского суда Московской области за 2019 г. Д. № 1-74.

же учетные записи, разъяснял правила и размещал публикации заданий для всех участников, включая Б. Кроме того, Г. пояснил суду, что участником созданной им беседы «На грани жизни» мог стать любой человек, ее посетивший; никого из участников созданной им беседы лично он не знал, относился ко всем одинаково, задания для всех участников были типовыми; какой-либо предвзятости, особого отношения либо неприязни ни к кому из участников беседы он не испытывал. Все это свидетельствует о едином умысле подсудимого и совершении преступления одним способом[1].

Действия Г. были квалифицированы как единое продолжаемое преступление, предусмотренное ч. 2 ст. 110^2 УК РФ (организация деятельности, направленной на побуждение к совершению самоубийства путем распространения информации о способах совершения самоубийства и призывов к совершению самоубийства, сопряженное с использованием информационно-телекоммуникационных сетей, включая сеть Интернет).

Кардинально противоположным примером квалификации аналогичных действий виновного является приговор Звериноголовского районного суда Курганской области.

Так, П., будучи пользователем общедоступной социальной сети «ВКонтакте», достоверно зная о повышенном интересе значительной части пользователей к темам самоубийства, депрессии и иного деструктивного контента (информации), в социальной сети «ВКонтакте» информационно-телекоммуникационной сети Интернет создал сообщество «Мантемореос», где умышленно в целях склонения лиц, в т. ч. несовершеннолетнего возраста, к совершению самоубийства путем уговоров и предложений и повышения уровня самооценки своей личности, самоутверждения себя как человека, способного руководить действиями других лиц, ***разместил общедоступную для***

[1] Архив Люберецкого городского суда Московской области за 2019 г. Д. № 1-74.

неограниченного круга пользователей *(выделено авт. — М. М.) социальной сети «ВКонтакте» информацию суицидального характера, а также данные своей электронной страницы «ВП», тем самым завлекая лиц, в т. ч. несовершеннолетних, имеющих намерения совершить суицид, вступить с ним в переписку с целью дальнейшего их склонения к совершению самоубийства.*

Далее в период с 27 августа по 22 сентября 2017 г. посредством использования социальной сети «ВКонтакте», действуя умышленно с целью склонения несовершеннолетних к совершению самоубийства путем уговоров и предложений и повышения уровня самооценки своей личности, самоутверждения себя как человека, способного руководить действиями других лиц, вступил в электронную переписку с А., которая сообщила ему, что является несовершеннолетней и находится в тяжелой жизненной ситуации. В ходе переписки, используя систематическое устойчивое целенаправленное психологическое воздействие, П. неоднократно давал указания и призывал ее к совершению последовательных агрессивных действий, а именно: наносить порезы на различные части тела, проникать в места, опасные для жизни, забираться на высотные здания. При этом П. осознавал и предвидел возможность лишения А. себя жизни и желал наступления этих последствий. П. вел с А. переписку в ночные и ранние утренние часы, т. е. во время, предназначенное для отдыха и сна, что являлось для последней дополнительной психотравмирующей нагрузкой, давал обязательные для выполнения задания, включающие обязательные просмотр и прослушивание аудио- и видеоматериалов, содержащих откровенные сцены насилия и осуществления людьми самоубийства разными способами, формирующие у потерпевшей депрессивную направленность сознания. Таким образом, П. умышленно совершил совокупность системных последовательных действий, направленных на склонение ее к совершению самоубийства.

Кроме того, в период с 27 августа по 14 сентября 2017 г., действуя с тем же умыслом, посредством использования социальной сети «ВКонтакте» П. вступил в электронную переписку с Е., также представившейся несовершеннолетней, в ходе которой совершил аналогичные действия в отношении нее.

Несмотря на то что в действиях П. изначально усматривается состав преступления, предусмотренного ч. 2 ст. 110^2 УК РФ, он был осужден по п. «а», «в», «д» ч. 3 ст. 110^1 УК РФ за склонение к совершению самоубийства путем уговоров, предложений при отсутствии признаков доведения до самоубийства, совершенное в отношении двух несовершеннолетних, в информационно-телекоммуникационных сетях (включая сеть Интернет), поскольку умысел организации деятельности, направленной на побуждение к совершению самоубийства, был направлен на дальнейшее склонение лиц, в т. ч. несовершеннолетнего возраста, к совершению самоубийства[1].

С учетом того, что цель организации такой деятельности состояла в завлечении неопределенного круга лиц, имеющих намерения совершить суицид, для дальнейшего их склонения к совершению самоубийства, квалификация действий виновного в данном приговоре является необоснованной.

Таким образом, анализ следственно-судебной практики свидетельствует об имеющихся проблемах в части квалификации преступных действий лиц, одновременно содержащих в себе признаки составов преступлений, предусмотренных п. «д» ч. 3 ст. 110^1 и ч. 2 ст. 110^2 УК РФ. Подобные действия должны квалифицироваться по совокупности указанных составов преступлений.

Подводя итог рассмотрению особенностей квалификации преступлений, инспирирующих суицид в информационно-телекоммуникационной сети Интернет, следует отметить, что разграничение составов преступлений, предусмотренных п. «д»

[1] Архив Звериноголовского районного суда Курганской области за 2019 г. Д. № 1-3.

ч. 2 ст. 110 и п. «д» ч. 3 ст. 110^1 УК РФ, в первую очередь следует производить по признакам объективной стороны. Основная суть склонения к самоубийству и доведения до самоубийства заключается в воздействии на потерпевшего, направленном на возбуждение (формирование) у этого лица желания к совершению суицида. Однако для склонения к самоубийству характерны интеллектуальные методы воздействия на потерпевшего, а для доведения до самоубийства — физические и/или психические формы насилия. Основное отличие содействия совершению самоубийства, позволяющее отграничивать его от склонения к самоубийству, заключается в том, что смысл его состоит в оказании помощи потерпевшему в совершении самоубийства, когда он уже принял решение о его совершении.

Доведение до самоубийства, склонение к самоубийству и содействие его совершению имеют адресный характер преступных действий и направленность на определенное лицо. В связи с тем, что организация деятельности, направленной на побуждение к совершению самоубийства, представляет собой неперсонифицированное воздействие, которое охватывает неопределенный круг лиц, в составе преступления, предусмотренного ст. 110^2 УК РФ, следует выделить дополнительный непосредственный объект — общественную безопасность, под которой понимается состояние защищенности общества от угроз информационного характера (пропаганды самоубийств).

Кроме того, квалификация действий лица, одновременно содержащих признаки составов преступлений, предусмотренных п. «д» ч. 3 ст. 110^1 и ч. 2 ст. 110^2 УК РФ, должна осуществляться по совокупности указанных преступлений.

Для того чтобы квалифицировать деяние по ч. 2 ст. 128^1 УК РФ, необходимо установить ряд обстоятельств, которые вызывают наибольшие трудности на практике: уяснить признаки сведений, распространяемых виновным, определить объективную сторону преступления и потерпевшего, усмотреть критерий «заведомость» в рамках субъективной стороны.

1. Сведения могут быть в электронном виде: текст, видео-, аудиофайл, изображение (картинка), фотоколлаж, созданный самим преступником или другим лицом, а также могут выражаться

в устной, письменной и других формах, передаваемых при помощи инструментов IP-телефонии (видео-, аудиосвязи).

Уголовный закон определяет, что распространяемые при клевете сведения должны обладать следующими характеристиками: во-первых, быть ложными, во-вторых, либо порочащими честь и достоинство лица, либо подрывающими его репутацию. В соответствии с п. 7 Постановления Пленума Верховного Суда Российской Федерации от 24.02.2005 № 3[1] к клеветническим сведениям относятся утверждения[2] о фактах[3] или событиях[4], которые не соответствуют действительности (поскольку не имели места в реальности во время, к которому относятся) и являются порочащими вследствие содержания одного из нижеизложенных умозаключений:

– о нарушении лицом действующего законодательства;

– совершении нечестного поступка;

– неправильном, неэтичном поведении в личной, общественной или политической жизни;

– недобросовестности при осуществлении производственно-хозяйственной и предпринимательской деятельности;

– нарушении деловой этики или обычаев делового оборота, которые умаляют честь и достоинство гражданина или его деловую репутацию.

Таким образом, распространяемые сведения могут касаться прошедших событий и настоящих. Распространение вымышлен-

---

[1] О судебной практике по делам о защите чести и достоинства граждан, а также деловой репутации граждан и юридических лиц: постановление Пленума Верховного Суда Российской Федерации от 24.02.2005 № 3 // Бюл. Верховного Суда Российской Федерации. 2005. № 4.

[2] Утверждение — положение, мысль, которой доказывают, утверждают что-нибудь. См.: Толковый словарь Ожегова онлайн. URL: https://slovarozhegova.ru/word.php?wordid=33438 (дата обращения: 08.05.2024).

[3] Факт — действительное, вполне реальное событие, явление; то, что действительно произошло, происходит, существует. См.: Толковый словарь Ожегова онлайн. URL: https://slovarozhegova.ru/word.php?wordid=33652 (дата обращения: 08.05.2024).

[4] Событие — то, что произошло, то или иное значительное явление, факт общественной, личной жизни. См.: Толковый словарь Ожегова онлайн. URL: https://slovarozhegova.ru/word.php?wordid=29578 (дата обращения: 08.05.2024).

ных предстоящих фактов или событий не влечет ответственности по ст. 128[1] УК РФ.

Некоторые суды дают пояснения: *«…распространяемые при клевете сведения должны в деталях либо в общих чертах характеризовать какой-либо конкретный факт, при этом они могут прямо указывать на событие или содержать косвенную информацию о нем»*[1].

Отметим, что сообщение правдивых (имеющих место) порочащих сведений так же, как и сообщение ложных (в т. ч. и с положительной окраской, например о совершении героического поступка) не порочащих сведений, не дает основания для квалификации действий по ч. 2 ст. 128[1] УК РФ, т. к. в этом случае не соблюдаются положения закона. Не наступит уголовная ответственность и тогда, когда лицо излагает правдивые сведения, а потерпевший считает их ложными (поскольку по истечении длительного времени забыл обстоятельства прошедших событий, не желает предавать их огласке, не разобрался в происходящих событиях и т. п.) и порочащими.

Так, Кирово-Чепецкий районный суд Кировской области оставил без изменений оправдательный приговор мирового судьи в отношении П-ва, который в ходе переписки со своей сестрой М. в «ВКонтакте» сообщил, что в прошлом ее мать П. (будучи сожительницей его отца) «предлагала ему повеситься, изводила криками и подставами». П. посчитала это клеветой и обратилась в суд. В ходе разбирательства было доказано, что П-в сообщил соответствующие действительности сведения. Когда он был малолетний, между ним и сожительницей отца П. после рождения их совместной дочери были конфликтные отношения. Однажды на вопрос П-ва: «Ну что мне еще нужно сделать?», она ответила: «Иди повесься!»[2]

[1] Архив Прикубанского районного суда г. Краснодара за 2019 г. Д. № 10-50/2019. URL: http://sudact.ru (дата обращения: 08.05.2024).

[2] Архив Кирово-Чепецкого районного суда Кировской области за 2020 г. Д. № 10-2/2020. URL: http://sudact.ru (дата обращения: 08.05.2024).

Или другое дело. *Пушкинский городской суд Московской области оставил без изменения оправдательный приговор мирового судьи в отношении О. В ходе разбирательства было установлено, что распространяемые О. письменные сообщения про Ю. не являлись для нее заведомо ложными, а были ее заблуждением относительно действительного хода событий*[1].

В пункте 7 Постановления Пленума Верховного Суда Российской Федерации от 24.02.2005 № 3 указывается, что не могут рассматриваться как не соответствующие действительности сведения, содержащиеся в судебных решениях и приговорах, постановлениях органов предварительного следствия и других процессуальных или иных официальных документах. Следовательно, даже когда названные документы изложены на сайтах сети Интернет, сведения, содержащиеся в них, не являются клеветническими.

Если утверждения не касаются каких-либо конкретных фактов, а лишь содержат абстрактную оценку типа «вредный человек», «слабый студент», «плохой сосед», то они не могут быть признаны порочащими сведениями[2].

На практике распространены примеры, когда на различных сайтах в сети Интернет в комментариях к какому-либо новостному сообщению человек оставляет негативное высказывание о деятельности должностных лиц. Во всех случаях для того, чтобы определить, являются ли сведения утверждением о фактах или событиях, носят ли порочащий характер или представляют субъективное мнение, правоприменителям необходимо назначать судебную (лингвистическую) экспертизу. Если в результате ее проведения будет установлено, что высказывание носит характер критики государственных должностных лиц

[1] Архив Пушкинского городского суда Московской области за 2019 г. Д. № 10-10/2019. URL: http://sudact.ru (дата обращения: 08.05.2024).

[2] Комментарий к Уголовному кодексу Российской Федерации (постатейный): в 4 т.; т. 2: Особенная часть. Разделы VII–VIII / А. В. Бриллиантов, А. В. Галахова, В. А. Давыдов [и др.]; отв. ред. В. М. Лебедев. М.: Юрайт, 2017 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

о выполнении ими своих обязанностей, а это согласно п. 9 Постановления Пленума Верховного Суда Российской Федерации от 24.02.2005 № 3 является допустимым с целью обеспечения надлежащего исполнения должностных полномочий, то ответственность по ч. 2 ст. 128[1] УК РФ не наступит.

Напротив, в том случае, когда экспертиза придет к мнению, что высказывание содержит утверждение о факте или событии, являющемся порочащим, то при установлении всех необходимых признаков состава клеветы действия виновного подлежат соответствующей юридической оценке.

2. Следующий обязательный признак — потерпевший. Согласно ст. 128[1] УК РФ оклеветать возможно либо другое лицо (ч. 1), либо нескольких лиц, в т. ч. индивидуально не определенных (ч. 2).

Несмотря на то что законодатель, помимо указания на «другое» лицо, больше никаких его признаков не обозначил, клевета, совершенная публично с использованием информационно-телекоммуникационных сетей, включая сеть Интернет, все же должна быть в отношении не абстрактного, а конкретного человека.

Так, апелляционным постановлением Октябрьского районного суда г. Мурманска был отменен обвинительный приговор мирового судьи, и уголовное дело прекращено вследствие установления, что В. в сети Интернет оклеветал неопределенное лицо, которое занимает должность руководителя. Фамилия потерпевшего или его персональные данные не упоминались. В ходе судебного следствия привлеченный специалист пояснила, что «из содержания обращения невозможно определить, в отношении какого конкретного лица в нем приведены сведения. Любое лицо, обладающее организационно-распорядительными функциями, относящееся к категории руководителей, в т. ч. руководитель какого-либо подразделения, прочитав это обращение, мог отнести его на свой счет»[1].

[1] Архив Октябрьского районного суда г. Мурманска за 2019 г. Д. № 10-20/2019.

Потерпевшим может выступать ребенок до достижения им 18 лет, лицо с физическими (глухой, слепой, находящийся в болезненном или бессознательном состоянии) или психическими нарушениями здоровья (слабоумие или другое психическое расстройство).

В науке уголовного права поднимают проблемный вопрос о признании потерпевшим умершего. Одни авторы поддерживают такую позицию[1], другие поясняют, что подобное возможно только в том случае, если распространяемые позорящие сведения об умершем задевают честь живых людей[2] (родственников), потому как раздел VII УК РФ охраняет личность, т. е. живого человека[3]. С последними доводами следует согласиться.

Поскольку ч. 2 ст. 128[1] УК РФ является преступлением публичного обвинения, то необязательно распространяемая в сети Интернет клевета должна быть доведена до сведения этого конкретного потерпевшего, достаточно ознакомления с ней любого (не потерпевшего) хотя бы одного человека. При таком механизме совершения преступления причиняется вред общественным отношениям, охраняющим честь[4] этого потерпевшего (объектом

---

[1] Подройкина И. А. Юридический анализ клеветы как уголовно наказуемого деяния // Наука и образование: хозяйство и экономика; предпринимательство; право и управление. 2020. № 2. С. 114; Уголовное право Российской Федерации. Особенная часть: учебник / Ю. В. Грачева, Л. Д. Ермакова, Г. А. Есаков [и др.]; под ред. Л. В. Иногамовой-Хегай, А. И. Рарога, А. И. Чучаева. 2-е изд., испр. и доп. М.: Контракт, Инфра-М, 2009 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Комментарий к Уголовному кодексу Российской Федерации (постатейный): в 4 т.; т. 2: Особенная часть. Разделы VII–VIII / А. В. Бриллиантов, А. В. Галахова, В. А. Давыдов [и др.]; отв. ред. В. М. Лебедев. М.: Юрайт, 2017 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

[3] Комментарий к Уголовному кодексу Российской Федерации (постатейный): в 2 т. / А. В. Бриллиантов, Г. Д. Долженкова, Э. Н. Жевлаков [и др.]; под ред. А. В. Бриллиантова. 2-е изд. М.: Проспект, 2015. Т. 1 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс»; Брагина А. Г. Клевета и смежные с ней составы преступления // Актуальные проблемы борьбы с преступлениями и иными правонарушениями: мат-лы девятой Междунар. научно-практ. конф-ции. Барнаул: БЮИ МВД России, 2011. Ч. 1. С. 134.

[4] Честь — общественная оценка личности человека как участника общественных отношений, нравственных и иных качеств. (См.: Комментарий к Уголовному кодексу Российской Федерации (постатейный): в 4 т.; т. 2: Особенная часть. Разделы VII–VIII / А. В. Бриллиантов, А. В. Галахова, В. А. Давыдов [и др.]; отв. ред.

преступления выступают честь, достоинство, деловая репутация[1]).

Нетипичной для УК РФ является формулировка квалифицирующего признака клеветы «в отношении нескольких лиц». Полагаем, что его необходимо вменять в том случае, если виновный совершил преступление в отношении двух и более потерпевших одновременно или в разное время. Сложнее дело обстоит с трактовкой понятия «в том числе индивидуально не определенных».

Большинство ученых справедливо отмечают, что для правоприменителя внесенная в УК РФ данная оценочная дефиниция создает проблемы доказывания объективной и/или субъективной сторон преступления, т. к. нет возможности установить круг потерпевших[2].

Тем не менее некоторые авторы предлагают различные варианты толкования названного признака, каким-либо образом конкретизирующие этот круг. Например, «конкретная группа лиц конкретной целевой аудитории, но без персонализации» (коллектив организации)[3]; «может идти речь о каких-либо партиях, общественных объединениях, политиках, чиновниках и других лицах, имена которых прямо не называются, но всем понятно, о ком идет речь»[4]; «конкретизация потерпевших происходит не по индивидуальным признакам (большое число имманентно

В. М. Лебедев. М.: Юрайт, 2017 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».)

[1] В этом случае могут возникнуть проблемы процессуального характера, связанные с доказыванием.

[2] См., например: Егорова Н. А. Новое в уголовно-правовом противодействии клевете // Законность. 2021. № 3 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс»; Дубовиченко С. Н., Карлов В. П. Клевета в сети «Интернет» и в отношении индивидуально-неопределенного круга лиц // Татищевские чтения: актуальные проблемы науки и практики: мат-лы XVIII Междунар. научно-практ. конф-ции (23–24 апреля 2021 г.): в 3 т. Тольятти, 2021. Т. 3. С. 151–156 и др.

[3] Ступина С. А. Мнение или клевета? Новое в статье 128.1 УК РФ // Актуальные проблемы борьбы с преступностью: вопросы теории и практики: мат-лы XXIV Междунар. научно-практ. конф-ции (8–9 апреля 2021 г.). Красноярск, 2021. Ч. 2. С. 186.

[4] Осадчая Н. Г. Клевета: особенности уголовно-правового регулирования // Наука и образование; хозяйство и экономика; предпринимательство: право и управление. 2021. № 2. С. 122.

присущих данной личности свойств, позволяющих отличить ее от любого другого человека на этой планете), а по одному — двум свойствам, ограничивающим групповую принадлежность»[1].

3. Объективная сторона преступления проявляется в виде активного действия. Согласно п. 7 Постановления Пленума Верховного Суда Российской Федерации от 24.02.2005 № 3 под распространением сведений в информационно-телекоммуникационных сетях, включая сеть Интернет, следует понимать их опубликование или сообщение в любой форме хотя бы одному лицу.

Отметим, что в теории и правоприменительной практике под опубликованием информации в информационно-телекоммуникационных сетях традиционно понимается ее размещение, а под сообщением — провозглашение (это возможно при помощи инструментов IP-телефонии).

Для квалификации действий виновного по ч. 2 ст. 128^1 УК РФ необходимо установить публичный способ распространения клеветы, например размещение ее на сайтах, форумах или в блогах, массовая рассылка электронных сообщений и иные подобные действия, в т. ч. рассчитанные на последующее ознакомление с информацией других лиц[2].

Вместе с тем в рамках уголовного дела необходимо доказать, что размещение клеветнических сведений публично было осуществлено конкретным лицом (к примеру, владельцем аккаунта или другим пользователем аккаунта, действовавшим не от своего имени (от имени другого человека или анонимно) и т. п.).

Так, в апелляционном постановлении Джанкойского районного суда Республики Крым была оправдана И. за отсутствием в ее действиях состава преступления, т. к.

[1] Григорьева Л. В. Критический обзор положений ст. 128.1 УК РФ // Вестник Саратовской государственной юридической академии. 2021. № 4 (141). С. 135.

[2] О судебной практике по уголовным делам о преступлениях экстремистской направленности [Электронный ресурс]: постановление Пленума Верховного Суда Российской Федерации от 28.06.2011 № 11 (ред. от 28.10.2021), п. 7. Доступ из справ.-правовой системы «КонсультантПлюс».

не было доказано, что именно она создала страницу в «Одноклассниках» под именем ФИО1 и размещала на ней ложные сведения, порочащие честь и достоинство потерпевшей[1].

Если преступник распространяет информацию в сети Интернет только тому человеку, которого они касаются, при этом исключается возможность ознакомления с ней третьих лиц, то ответственность по ч. 2 ст. 128[1] УК РФ не наступит[2].

При размещении ложных, порочащих сведений на сайте, зарегистрированном в качестве средства массовой информации (далее — СМИ)[3] (например, в сетевом издании), можно вменять ч. 2 ст. 128[1] УК РФ, но в описательно-мотивировочной части следует указать «клевета, содержащаяся в средствах массовой информации».

Следует также отметить, что само по себе обращение в государственные органы и органы местного самоуправления, в котором приводятся сведения о предполагаемом, совершенном либо готовящемся преступлении, не является преступным, поскольку соответствует положениям Федерального закона «О порядке рассмотрения обращений граждан Российской Федерации»[4]. Выяснение же того, было ли такого рода обращение в указанные органы обусловлено стремлением (попыткой) реализовать свои конституционные права или оно связано исключительно с намерением причинить вред другому лицу, подлежит установлению на основе фактических обстоятельств в каждом конкрет-

[1] Архив Джанкойского районного суда Республики Крым за 2020 г. Д. № 10-1/2020. URL: http://sudact.ru (дата обращения: 08.05.2024).

[2] О судебной практике по делам о защите чести и достоинства граждан, а также деловой репутации граждан и юридических лиц: постановление Пленума Верховного Суда Российской Федерации 24.02.2005 № 3, п. 7 // Бюл. Верховного Суда Российской Федерации. 2005. № 4.

[3] См.: О средствах массовой информации [Электронный ресурс]: Закон Российской Федерации от 27.12.1991 № 2124-1, ст. 2. Доступ из справ.-правовой системы «КонсультантПлюс».

[4] О порядке рассмотрения обращений граждан Российской Федерации [Электронный ресурс]: федеральный закон Российской Федерации от 02.05.2006 № 59-ФЗ (ред. от 04.08.2023). Доступ из справ.-правовой системы «КонсультантПлюс».

ном случае, имеется в виду недопустимость установления судом лишь формальных условий применения нормы[1].

В частности, обвинительный приговор за клевету в отношении К. в апелляционной инстанции был оставлен без изменения. В ходе судебного разбирательства было установлено, что К. ... *во избежание наступления вредных для себя последствий… от поданного в отношении нее Д. заявления в полицию о привлечении к уголовной ответственности за вывоз имущества из принадлежащей ему квартиры решила опорочить его честь и достоинство. Поскольку Д. работал… заместителем руководителя администрации Ступинского муниципального района — руководителем аппарата…, для реализации своих намерений она направила письменные обращения… в администрацию Ступинского муниципального района <адрес>, а также в ОМВД России по <адрес>, а также электронные обращения… на официальные сайты ГУ МВД России по <адрес> на имя начальника ФИО10 и МВД России на имя Министра внутренних дел Российской Федерации ФИО11; интернет-портал Аппарата Правительства Российской Федерации на имя Председателя Правительства Российской Федерации ФИО12…, в которых изложила не соответствующие действительности порочащие сведения о Д.*[2]

Момент окончания преступления, предусмотренного ч. 2 ст. 128[1] УК РФ, зависит от вида распространяемых сведений. Если это электронная информация, то преступление окончено в момент ее публикации (размещения), т. е. когда появляется возможность у любого человека с ней ознакомиться. Клевета,

[1] Об отказе в принятии к рассмотрению жалобы гражданина Москалева Михаила Васильевича на нарушение его конституционных прав частью первой статьи 128.1 Уголовного кодекса Российской Федерации и статьей 318 Уголовно-процессуального кодекса Российской Федерации [Электронный ресурс]: определение Конституционного Суда Российской Федерации от 05.12.2019 № 3272-О. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Архив Ступинского городского суда Московской области за 2014 г. Д. № 10-19/2014. URL: http://sudact.ru (дата обращения: 08.05.2024).

передающаяся при помощи инструментов IP-телефонии, окончена с момента осуществления видео-, аудиозвонка, когда у третьего лица (не потерпевшего) возникает возможность ее воспринять.

В теории уголовного права можно встретить мнение, что клевета, размещенная на сайте в сети Интернет, если она впоследствии не обновлялась, признается длящимся преступлением и, следовательно, оканчивается в момент ее ликвидации с сайта[1]. Однако правоприменительная практика в подобном случае идет по пути признания преступления оконченным в момент публикации (размещения) клеветнических сведений на сайте.

При клевете в сети Интернет в отношении одного и того же потерпевшего несколько раз с единым умыслом содеянное не подлежит совокупности преступлений и необходимо вменять ч. 2 ст. 128[1] УК РФ.

В том случае, когда виновный в отношении одного и того же потерпевшего клевещет в сети Интернет несколько раз и каждый раз у него возникает умысел вновь, необходимо вменять несколько эпизодов ч. 2 ст. 128[1] УК РФ по признаку «клевета, совершенная публично с использованием информационно-телекоммуникационных сетей, включая сеть Интернет».

Возможно и покушение на клевету, когда набран текстовый файл, смонтирован видеофайл, записан аудиофайл, создано изображение (картинка) или фотоколлаж, которые содержат ложные и порочащие сведения и сохранены в памяти электронного носителя информации с умыслом в дальнейшем их распространить, но по независящим от лица обстоятельствам задуманное не удалось осуществить.

Если клевета, совершенная публично с использованием информационно-телекоммуникационных сетей, включая сеть Интернет:

[1] Аниськина Э. Г. Кибер-клевета: проблемы квалификации // Уголовный закон в эпоху искусственного интеллекта и цифровизации: сб. тр. по мат-лам Всерос. научно-практ. конф-ции с междунар. участием в рамках I Саратовского междунар. юрид. форума, посв. 90-летнему юбилею Саратовской государственной юридической академии (Саратов, 9 июня 2021 г.). Саратов, 2021. С. 132.

– осуществляется с использованием служебного положения, то ответственность наступает по ч. 3 ст. 128[1] УК РФ;

– касается сведений о том, что лицо страдает заболеванием, представляющим опасность для окружающих, — по ч. 4 ст. 128[1] УК РФ;

– соединена с обвинением лица в совершении преступления против половой неприкосновенности и половой свободы личности либо тяжкого или особо тяжкого преступления — по ч. 5 ст. 128[1] УК РФ.

Обращение (подача заявления на официальном сайте) в органы, осуществляющие уголовное преследование, и к мировому судье с ложной информацией о совершении другим человеком преступления с умыслом привлечь такового к уголовной ответственности подлежит квалификации по ст. 306 УК РФ.

Если при совершении вымогательства виновный угрожает распространить клеветнические сведения, то его действия подлежат квалификации по ст. 163 УК РФ. При дальнейшем непосредственном осуществлении этой угрозы требуется совокупность ст. 163 и 128[1] УК РФ[1]. Также ответственности по двум составам преступления — ст. 128[1] и ст. 319 УК РФ — будет подлежать лицо, которое оклеветало представителя власти и его же оскорбило, используя информационно-телекоммуникационные сети.

Клевету, распространенную в сети Интернет в отношении судьи, присяжного заседателя, прокурора, следователя, лица, производящего дознание, сотрудника органов принудительного исполнения Российской Федерации относительно их непосредственной деятельности, надлежит оценивать по соответствующей части ст. 298[1] УК РФ.

В юридический литературе представлено мнение, согласно которому клевета, направленная на возбуждение ненависти или вражды, совершенная по мотивам политической, идеологической, расовой, национальной или религиозной ненависти или вражды либо по мотивам ненависти или вражды в отношении

[1] О судебной практике по делам о вымогательстве [Электронный ресурс]: постановление Пленума Верховного Суда Российской Федерации от 17.12.2015 № 56, п. 12. Доступ из справ.-правовой системы «КонсультантПлюс».

какой-либо социальной группы, должна квалифицироваться по ст. 282 УК РФ[1].

4. Субъективная сторона ч. 2 ст. 128[1] УК РФ характеризуется умышленной формой вины. При этом необходимо установить признак «заведомость», который предполагает, что, совершая деяние, субъект осознает общественную опасность своих действий, понимает ложность распространяемых сведений (точно знает о ложности сообщаемых им сведений[2]), а также то, что эти сведения порочат честь, достоинство другого лица, подрывают его репутацию[3].

Если преступник уверен, что распространяет правдивую информацию, хотя на самом деле она ложная, т. е. добросовестно заблуждается относительно соответствия ее действительности, то он не может нести ответственность за клевету[4].

Таким образом, для правильной квалификации клеветы, совершенной публично с использованием информационно-телекоммуникационных сетей, включая сеть Интернет, необходимо учитывать ряд моментов:

1. Предмет преступления — клеветнические сведения — должен обладать следующими характеристиками: быть ложным, порочить честь и достоинство другого лица либо подрывать его репутацию.

2. Объективная сторона деяния, предусмотренного ч. 2 ст. 128[1] УК РФ, проявляется в виде публичного способа распространения клеветы, например размещения ее на сайтах, форумах или в бло-

---

[1] Ступина С. А. Отдельные вопросы квалификации клеветы // Эпоха науки. 2021. № 25. С. 141.

[2] Комментарий к Уголовному кодексу Российской Федерации (постатейный): в 4 т.; т. 2: Особенная часть. Разделы VII–VIII / А. В. Бриллиантов, А. В. Галахова, В. А. Давыдов [и др.]; отв. ред. В. М. Лебедев. М.: Юрайт, 2017 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

[3] Комментарий к Уголовному кодексу Российской Федерации (постатейный): в 2 т. / А. В. Бриллиантов, Г. Д. Долженкова, Э. Н. Жевлаков [и др.]; под ред. А. В. Бриллиантова. 2-е изд. Т. 1; Архив Якутского судебного участка № 40 Республики Саха (Якутия) за 2017 г. Д. № 1-1/2017.

[4] Подройкина И. А. Юридический анализ клеветы как уголовно наказуемого деяния // Наука и образование: хозяйство и экономика; предпринимательство; право и управление. 2020. № 2. С. 116; Архив Шатурского городского суда Московской области от 15.10.2020. Д. № 10-7/2020. URL: http://sudact.ru (дата обращения: 08.05.2024).

гах, массовой рассылки электронных сообщений и иных подобных действиях, в т. ч. рассчитанных на последующее ознакомление с информацией других лиц. Вместе с тем в рамках уголовного дела необходимо доказать, что размещение клеветнических сведений публично было осуществлено конкретным лицом (к примеру, владельцем аккаунта или другим пользователем аккаунта, действовавшими не от своего имени (от имени другого человека или анонимно), и т. п.).

3. Момент окончания преступления зависит от вида распространяемых сведений. Если это электронная информация, то преступление окончено в момент ее публикации (размещения), т. е. когда появляется возможность у третьего лица с ней ознакомиться. Клевета, передающаяся при помощи инструментов IP-телефонии, окончена с момента осуществления видео-, аудиозвонка, когда у третьего лица возникает возможность ее воспринять.

2.2. Уголовно-правовое предупреждение преступлений в сфере экономики, совершаемых с использованием информационно-телекоммуникационных технологий

Анализ Особенной части УК РФ показывает, что именно преступления в сфере экономики наиболее часто совершаются с использованием IT-технологий. Вследствие этого нормы раздела VIII в последние годы подвергались значительным изменениям. Безусловно, указанный раздел является достаточно объемным и включает в себя 84 состава преступления, в связи с чем интерес в рамках данного исследования представляют лишь проблемные с точки зрения квалификации и толкования составы.

Особые сложности возникают при квалификации *кражи с банковского счета, а равно в отношении электронных денежных средств* (п. «г» ч. 3 ст. 158 УК РФ).

Рассматриваемый квалифицированный состав выделен по особенностям предмета преступления, толкование которого представляется достаточно затруднительным.

Выделение такого вида предмета преступления предопределило изменение представления об имуществе в рамках составов хищений исключительно как физического предмета, что, по нашему мнению, является новым направлением, развивающим традиционное учение о формах и видах хищения.

В научной литературе в отдельных исследованиях отождествляются электронные деньги и безналичные[1].

Отдельными авторами предлагаются критерии разграничения обозначенных понятий. Например, А. В. Архипов разделяет понятия «электронные» и «безналичные денежные средства»[2].

Поддерживая обозначенную позицию, отметим, что понятие безналичных денег в законодательстве отсутствует. Однако в соответствии со ст. 140 ГК РФ платежным средством на территории РФ выступает рубль. При этом платежи могут осуществляться путем наличных и безналичных расчетов. Статья 861 ГК РФ определяет порядок безналичных расчетов, осуществляемых путем перевода банком денежных средств, находящихся на счете конкретного лица. Таким образом, безналичные деньги всегда «привязаны» к счету.

Иное содержание включают в себя электронные деньги. В Федеральном законе Российской Федерации от 27.06.2011 № 161-ФЗ «О национальной платежной системе»[3] под ними понимаются денежные средства, которые предварительно предоставлены одним лицом другому без открытия банковского счета. Очевидно, что в отличие от безналичных электронные деньги могут располагаться вне банковского счета в любых платежных системах.

При этом если судебная практика по безналичным денежным средствам достаточно устоявшаяся, то правовая природа электронных денег вызывает в научной литературе дискуссии. В частности, остается неясным, следует ли относить к электрон-

[1] См.: Байбарин А. А., Садчикова Д. Н. Кража безналичных и электронных денег: об актуальных проблемах правоприменения // Вестник Сургутского государственного университета. 2022. № 1 (35). С. 60-68.

[2] Архипов А. В. Ответственность за хищение безналичных и электронных денежных средств: новеллы законодательства // Уголовное право. 2018. № 3. С. 4–9.

[3] Российская газета. 2011. 30 июня. № 139.

ным денежным средствам криптовалюту, бонусы торговых организаций и т. д. Решение обозначенной проблемы возможно только путем внесения изменений в уголовное законодательство и определения статуса таких средств платежа[1].

Не отличается единообразием размер электронных денег, необходимый для привлечения виновного к уголовной ответственности[2]. Исходя из предписания, закрепленного в ст. 7.27 КоАП РФ, наличие квалифицированного состава нивелирует значение размера похищенного предмета. Однако во многих регионах РФ отказывают в возбуждении уголовного дела, если денежная сумма менее 500, 1000 рублей и т. д.

В отдельных случаях судом вообще не усматривается наличие электронных денежных средств. В частности, такая ситуация имеет место при снятии по чужой карте денег посредством банкомата.

> *Например, Ю., зная пин-код от банковской карты Ш., снял посредством банкомата 5000 рублей. По мнению Судебной коллегии по уголовным делам Красноярского краевого суда, квалификация по п. «г» ч. 3 ст. 158 УК РФ проведена неверно, поскольку данный признак имеется только при хищении в рамках формы безналичных расчетов*[3].

Полагаем, что ограничение действия п. «г» ч. 3 ст. 158 УК РФ исключительно сферой безналичных расчетов и переводов денежных средств виновным по своему усмотрению не соответствует целям введения данного квалифицированного состава. В связи с этим предлагаем осуществлять квалификацию по дан-

---

[1] Ермакова О. В. Мошенничество с использованием электронных средств платежа: вопросы толкования и разграничения со смежными составами // Актуальные проблемы уголовного законодательства на современном этапе: сборник науч. тр. Междунар. научно-практ. конф-ции (Волгоград, 17 мая 2019 г.). Волгоград: Тип. ИП «Слободчикова А. Д.», 2019. С. 128–131.

[2] Клименко А. К. Хищения безналичных и электронных денежных средств: вопросы квалификации // Российский следователь. 2020. № 5. С. 38–42.

[3] Апелляционное определение Красноярского краевого суда от 18 декабря 2018 г. по делу № 22-7584/2018 // Сайт Красноярского краевого суда. URL: https://kraevoy--krk.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=7998836&delo_id=4&new=4&text_number=1 (дата обращения: 08.05.2024).

ному квалифицирующему признаку как в случаях безналичных расчетов, так и при использовании банковской карты, не принадлежащей виновному.

Однако с целью разрешения вопросов соответствия этого предложения нормам уголовного закона, полагаем, необходимо дополнить содержание квалифицированного состава, закрепленного в п. «г» ч. 3 ст. 158 УК РФ, указанием на альтернативный способ в виде использования электронного средства платежа, под которым следует понимать электронные кошельки и предоплаченные банковские карты, предназначенные для перевода электронных денежных средств.

Обязательным признаком кражи электронных денег выступает способ, т. е. тайность изъятия и обращения данного предмета.

Анализ судебной практики позволяет выделить типичные ситуации тайного хищения, позволяющие унифицировать судебную практику по применению п. «г» ч. 3 ст. 158 УК РФ.

1 ситуация. Виновное лицо осуществляет перевод денежных средств безналичным способом с использованием необходимой информации держателя карты. При этом данная информация могла быть известна ему заранее либо получена любым способом от самого потерпевшего.

2 ситуация. Оплата покупки чужой картой при отсутствии обмана. Виновный может найти банковскую карту, а также похитить ее у собственника.

3 ситуация. Хищение посредством «Мобильного банка», когда потерпевший, подключая услугу, неверно сообщил номер телефона, присоединив принадлежащую ему банковскую карту к чужому номеру. В свою очередь, виновный, воспользовавшись этим, перевел денежные средства с расчетного счета потерпевшего[1].

При этом ранее судебная практика квалифицировала подобные случаи хищения с использованием «Мобильного банка» либо «СберБанк Онлайн» как мошенничество в сфере компьютерной информации, объясняя данное решение наличием способа

[1] Проблемы квалификации отдельных видов преступлений: учебное пособие / О. В. Ермакова, И. В. Ботвин, Л. Я. Тарасова [и др.]. Барнаул, 2021. С. 12.

в виде ввода, иного вмешательства в средства хранения, обработки компьютерной информации.

Так, Ч. в отделении СберБанка нашел в мусорном контейнере чек, содержащий конфиденциальную, не предназначенную для пользования компьютерную информацию, а именно логин и пароль для входа в «СберБанк Онлайн», на имя ранее ему незнакомого К. Реализуя свой преступный умысел на хищение чужого имущества путем вмешательства в средства хранения компьютерной информации, Ч. осуществил перевод денежных средств[1].

Полагаем, изменение в судебной практике квалификации таких действий и вменение не ст. 159[6], а п. «г» ч. 3 ст. 158 УК РФ абсолютно обосновано, поскольку все перечисленные частные случаи объединяет тайный способ изъятия, что полностью соответствует составу кражи.

Нельзя не обратить внимания на то, что Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 конкретизировало момент окончания данного преступления. Так, если предметом являются электронные денежные средства, то хищение признается оконченным с момента изъятия денег с банковского счета. Такие разъяснения были внесены в обозначенный документ только 29 июня 2021 г., а до этого момента для признания кражи электронных денег оконченной требовалось получение виновным этих денег в свое обладание, т. е. приобретение возможности пользоваться или распоряжаться похищенным.

Учитывая, что перевод денег может в отдельных случаях осуществляться длительный период времени, задержание виновного до момента завершения операции подлежало квалификации как покушение со ссылкой на ч. 3 ст. 30 УК РФ с назначением наказания с ограничением ¾ санкции статьи. Полагаем, такое решение не соответствует конструкции состава хищения (примечание 1 к ст. 158 УК РФ), поскольку момент окончания по пря-

[1] Приговор Самарского областного суда. URL: https://rospravosudie.com/court-sudebnyj-uchastok-88-samarskoj-oblasti-s/act-239015612 (дата обращения: 08.05.2024).

мому указанию закона должен связываться с причинением имущественного ущерба собственнику, который наступает в момент снятия денег у него со счета. В свою очередь, факт зачисления их на счет виновного для потерпевшего в принципе безразличен. Поэтому изменение разъяснений Верховным Судом РФ момента окончания хищения применительно к особому предмету в виде электронных денег следует признать обоснованным и правильным.

При разъяснении вопросов квалификации нельзя не акцентировать внимание на проблеме отграничения единичного продолжаемого хищения и совокупности преступлений. Так, на практике вызывает вопросы квалификация действий при совершении покупок по одной и той же похищенной или найденной карте.

Полагаем, что в первую очередь необходимо установить наличие единого умысла на совершение тождественных действий. Только тогда возможно утверждать о продолжаемом преступлении. Например, такая ситуация имеется в случае, если виновный сообщает о желании потратить все средства на полученной банковской карте. Если же умысел конкретизированный, направлен на хищение определенной суммы, а повторный факт совершается с вновь возникшим умыслом, то налицо совокупность преступлений (к примеру, лицо похищает карту только для расчета за проезд и долгое время не пользуется ею).

Среди всех специальных составов мошенничества разновидность, закрепленная в ст. 159^3 УК РФ *(мошенничество, совершенное с использованием электронных средств платежа)*, выступает наиболее сложной для толкования и правоприменения. Это объясняется тем, что диспозиция ч. 1 ст. 159^3 УК РФ лишь называет деяние, не отражает признаки, ему присущие.

При этом в первоначальной редакции 2012 г. данная диспозиция содержала указание на способ — обман уполномоченного работника кредитной, торговой, иной организации. Исключение в последующей редакции из диспозиции способа совершения преступления дестабилизировало судебную практику, а после введения квалифицирующего признака, предусмотренного п. «г» ч. 3 ст. 158 УК РФ, вообще привело к неприменению ст. 159^3 УК РФ.

По справедливому замечанию А. В. Архипова, «ст. 159^3 УК РФ не была исключена из УК РФ, а значит, имеются все основания полагать, что действия, составлявшие объективную сторону рассматриваемого преступления при предыдущей редакции ст. 159^3 УК РФ, по-прежнему должны квалифицироваться по данной норме»[1].

При разграничении составов преступлений, предусмотренных ст. 158, 159^3 и 159^6 УК РФ, необходимо исходить из особенностей способа совершения хищения. Так, для мошенничества характерны такие способы, как обман или злоупотребление доверием, в соответствии с которыми виновный сообщает заведомо ложные сведения или умалчивает о них, либо использует особые доверительные отношения при совершении преступления.

При отсутствии обмана или злоупотребления доверием действия виновного следует квалифицировать по п. «г» ч. 3 ст. 158 УК РФ.

Например, такая квалификация должна иметь место при хищении посредством «Мобильного банка», когда потерпевший, подключая услугу, неверно сообщил номер телефона, присоединив, принадлежащую ему банковскую карту к чужому номеру. В свою очередь, виновный, воспользовавшись этим, перевел денежные средства с расчетного счета потерпевшего[2].

Однако судебная практика не всегда руководствуется такими правилами.

Так, по приговору Братского городского суда Иркутской области А. был признан виновным в совершении деяния, предусмотренного ч. 2 ст. 159^3 УК РФ. Согласно материалам уголовного дела А., нашедший на барной стойке

[1] Архипов А. В. Мошенничество с использованием электронных средств платежа (ст. 159.3 УК РФ) // Уголовное право. 2019. № 5. С. 16–20.

[2] Ермакова О. В. Мошенничество с использованием электронных средств платежа: вопросы толкования и разграничения со смежными составами // Актуальные проблемы уголовного законодательства на современном этапе: сборник науч. тр. Междунар. научно-практ. конф-ции (Волгоград, 17 мая 2019 г.). Волгоград: Тип. ИП «Слободчикова А. Д.», 2019. С. 128–131.

чужую банковскую карту, оплачивал с ее помощью товары и услуги в нескольких магазинах[1].

Что касается разграничения специальных составов мошенничества, то, по нашему мнению, ст. 159^6 УК РФ (мошенничество в сфере компьютерной информации) содержит дополнительный способ в виде ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, наличие которого позволяет квалифицировать деяние по данной норме. Следовательно, мошенничество с использованием электронных денежных средств при наличии специального способа, конкретизированного в ст. 159^6 УК РФ, исключает квалификацию преступления по ст. 159^3 УК РФ.

В свете развития новых информационных средств, внедряющихся в сферы сделок с электронной валютой, функционирования интернет-магазинов, банковского обслуживания, дистанционных услуг продолжает оставаться актуальным *мошенничество в сфере компьютерной информации* (ст. 159^6 УК РФ). Вместе с тем правоприменительная практика сталкивается с серьезными проблемами, связанными с квалификацией мошенничеств, совершенных в рассматриваемой сфере.

Например, случаи использования онлайн-сервиса «Мобильный банк» в целях совершения хищения в судебной практике долгое время не находили единого подхода.

Так, в г. Брянске гражданин П. в целях хищения чужих денежных средств посредством СМС-сообщений на номер «900» перевел денежные средства с банковского счета потерпевшего на подконтрольный ему абонентский номер. Суд, изучив материалы уголовного дела, признал гражданина П. виновным по п. «в» ч. 2 ст. 158 УК РФ (Хищение

[1] Приговор Братского городского суда Иркутской области от 09.06.2020 по делу № 1-196/2020. URL: https://bsr.sudrf.ru/bigs/portal.htm (дата обращения: 08.05.2024).

денежных средств с причинением значительного ущерба гражданину)[1].

В Ульяновской области аналогичные действия суд оценил иначе, вменив подсудимому ч. 1 ст. 159[6] *УК РФ. Суд полагал, что, отправив СМС-сообщение на соответствующий номер, виновный осуществил ввод компьютерной информации, являющийся способом совершения мошеннических действий по ст. 159*[6] *УК РФ*[2].

Пленум Верховного Суда РФ вовремя обратил внимание на возникающие противоречия и в п. 21 Постановления от 30.12.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» разъяснил, что в случаях, когда хищение чужого имущества осуществляется путем использования учетных данных собственника или иного владельца имущества независимо от способа получения доступа к этим данным без незаконного воздействия на программное обеспечение, такие действия следует квалифицировать по ст. 158 УК РФ.

Вместе с тем вопросы отграничения мошенничества в сфере компьютерной информации от кражи остались и продолжают вызывать недопонимание как со стороны правоприменителя, так и со стороны научного сообщества. Дело в том, что сама редакция ст. 159[6] УК РФ противоречит определению мошенничества, закрепленному в ст. 159 УК РФ, поскольку не содержит указание на такие способы, как обман и злоупотребление доверием.

Отойдя от классического понимания мошенничества, законодатель, по сути, создал новый вид хищения, который осуществляется путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

---

[1] Архив Володарского районного суда г. Брянска. Приговор от 22.12.2016 по делу № 1-274/2016. URL: http://volodarsky.brj.sudrf.ru/ (дата обращения: 08.05.2024).

[2] Архив Димитровградского городского суда Ульяновской области. Приговор от 22.08.2017 по делу № 1-256/2017. URL: http://dimitrovgradskiy.uln.sudrf.ru/ (дата обращения: 08.05.2024).

В этом вопросе интерес представляет мнение Р. Ю. Шергина, который утверждает, что в данном случае любые другие формы хищений (в частности, кража, присвоение и растрата), в ходе совершения которых происходит применение компьютерного устройства для решения каких-либо второстепенных преступных задач (взлом цифрового замка хранилища, отключение его от охранной системы, отправка бухгалтерских или иных хозяйственных документов на вверенное имущество по электронной почте и т. п.), подпадают под признаки преступления, содержащегося в ст. 159[6] УК РФ[1]. От подобных решений в ходе квалификации деяний правоприменителя, вероятно, останавливает сам термин «мошенничество», не позволяющий квалифицировать по данной статье иные виды хищений. По большому счету это единственная функция такой редакции рассматриваемой статьи.

Однако сама идея на установление ответственности за хищения в сфере компьютерной (цифровой) информации достаточно актуальна и имеет право на существование. При этом научное сообщество неоднократно приходило к идее о создании такой нормы взамен существующей в ст. 159[6] УК РФ.

Р. Б. Иванченко и А. Н. Малышев считают необоснованной криминализацию деяния, предусмотренного в ст. 159[6] УК РФ, и полагают, что в уголовном законе следует предусмотреть статью «Хищение с использованием компьютерной информации», в которой установить ответственность за хищение чужого имущества или обращение права на чужое имущество в пользу виновного или третьих лиц вне зависимости от способа хищения, если при этом происходит вмешательство в компьютерную информацию или информационно-коммуникационные сети[2]. Аналогичной точки зрения придерживается И. А. Мусьял[3].

По нашему мнению, указанное предложение вполне закономерно и укладывается в современные тенденции законодателя,

---

[1] Шергин Р. Ю. Уголовная ответственность за компьютерное мошенничество: новое не всегда лучшее // Законность. 2017. № 5. С. 47–49.

[2] Иванченко Р. Б., Малышев А. Н. Проблемы квалификации мошенничества в сфере компьютерной информации // Вестник Воронежского института МВД России. 2014. № 1. С. 194–200.

[3] Мусьял И. А. Дифференцированные виды мошенничества: теоретические и практические проблемы: дис. ... канд. юрид. наук. Курск, 2018. С. 13.

однако представляется целесообразным в названии статьи сделать указание на использование цифровой информации, поскольку сфера действия предполагаемой статьи будет распространяться не только на компьютерную информацию, а более широкую (цифровую) сферу. Анализируя данную проблему, И. Р. Бегишев справедливо предлагает такое название статьи, как «Хищение с использованием компьютерной информации»[1].

Возвращаясь к действующей редакции ст. 159[6] УК РФ, следует отметить еще одну существенную проблему, которая заключается в отграничении деяний, содержащихся в диспозиции рассматриваемой статьи, от преступлений главы 28 УК РФ. Дело в том, что законодатель в ч. 1 ст. 159[6] УК РФ использует формулировки из посягательств в сфере компьютерной информации — ввод, удаление, блокирование, модификация компьютерной информации, иное вмешательство, а в главе о компьютерных преступлениях (за исключением ст. 274[2] УК РФ) — уничтожение, блокирование, модификация либо копирование компьютерной информации.

Налицо пересечение признаков состава мошенничества в сфере компьютерной информации со ст. 272-274[1] УК РФ при условии, что «уничтожение» и «удаление» — это синонимичные понятия.

Казалось бы, Пленум Верховного Суда в п. 20 постановления № 48 поставил точку в этом вопросе, определив, что мошенничество в сфере компьютерной информации, совершенное посредством неправомерного доступа к компьютерной информации или посредством создания, использования и распространения вредоносных компьютерных программ, требует дополнительной квалификации по статьям 272, 273 или 274[1] УК РФ. Однако ряд вопросов так и остается нерешенным[2].

---

[1] Бегишев И. Р. Некоторые вопросы противодействия мошенничеству в сфере компьютерной информации // Вестник Казанского юридического института МВД России. 2016. № 3. С. 112–117.

[2] См., например: Лопашенко Н. А. Компьютерное мошенничество – новое слово в понимании хищения или ошибка законодателя? // Пермский юридический альманах. 2019. № 2. С. 598–609; Шарапов Р. Д. Актуальные вопросы квалификации новых видов мошенничества // Проблемы квалификации и расследования преступ-

С созданием вредоносных программ, с помощью которых виновный совершает мошенничество в сфере компьютерной информации, всё достаточно логично и обоснованно. Преступник выполняет две объективные стороны: сначала создает и (или) использует вредоносную программу для хищения денежных средств, а затем совершает преступление, предусмотренное ст. 159^6 УК РФ. Вместе с тем Пленум Верховного Суда РФ не уточнил, по какой части ст. 273 УК РФ требуется дополнительная квалификация. Исходя из содеянного, следуя общей теории квалификации, речь должна идти о ч. 2 ст. 273 УК РФ (совершенные из корыстной заинтересованности), поскольку программа используется для компьютерного мошенничества.

Существует неоднозначная позиция о дополнительной квалификации мошенничества в сфере компьютерной информации и в ст. 272 УК РФ. В случае реальной совокупности, когда виновный вначале осуществляет неправомерный доступ к компьютерной информации, что влечет ее уничтожение, блокирование, модификацию либо копирование, а затем у него возникает умысел на совершение хищения денежных средств путем, к примеру, ввода новой информации либо модификации существующей, такие действия следует оценивать по ст. 159^6 и 272 УК РФ.

В ином случае, когда преступник одним действием совершает неправомерный ввод, удаление, блокировку либо модификацию компьютерной информации и это влечет незаконное получение им чужого имущества, такое деяние должно квалифицироваться лишь по ст. 159^6 УК РФ, поскольку в диспозиции статьи предусмотрена ответственность и за «иное вмешательство» в цифровые носители. Другими словами, последствиями в ст. 159^6 УК РФ является наступление имущественного ущерба путем манипуляций с компьютерной информацией, а последствиями в ст. 272 УК РФ являются эти же манипуляции (при этом способ совершения преступления на квалификацию не влияет).

Представляется, что в рассмотренном примере неправомерный доступ к охраняемой законом компьютерной информации (пусть

лений, подследственных органам дознания: мат-лы Всеросс. научно-практ. конфции. Тюмень, 2013. С. 3–5.

и повлекший уничтожение, блокирование, модификацию либо копирование компьютерной информации) является способом совершения преступления, предусмотренного ст. 159^6 УК РФ.

В противном случае есть серьезный риск наказать дважды за одно и то же преступление, при том что санкция по ч. 1 ст. 159^6 УК РФ содержит максимальное наказание в виде 4 месяцев ареста, а по ч. 1 ст. 272 УК РФ — 2 года лишения свободы.

Однако Пленум Верховного Суда и в этой проблеме поставил точку, разъяснив в новом Постановлении от 15.12.2022 № 37, что «мошенничество в сфере компьютерной информации (статья 159^6 УК РФ), совершенное посредством неправомерного доступа к компьютерной информации или посредством создания, использования и распространения вредоносных компьютерных программ, требует дополнительной квалификации по статье 272, 273 или 274^1 УК РФ»[1].

Таким образом, рассмотренные проблемы по вопросам применения статьи о мошенничестве в сфере компьютерной информации позволят правоприменителю избежать ошибок при оценке преступных деяний, связанных с мошенничеством в сфере компьютерной информации.

2.3. Уголовно-правовое предупреждение преступлений в сфере компьютерной информации

В число вопросов, требующих особого внимания при анализе проблем квалификации и толкования преступлений, совершаемых с использованием современных цифровых средств, несомненно, входят преступления, предусмотренные главой 28 УК РФ, а именно ст. 272-274^2.

[1] 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» [Электронный ресурс]: постановление Пленума Верховного Суда Российской Федерации от 15.12.2022 № 37. Доступ из справ.-правовой системы «КонсультантПлюс».

При обращении к названию главы 28 УК РФ становится очевидным, что для квалификации преступлений принципиальное значение имеет предмет, в качестве которого выступает компьютерная информация, представляющая собой сведения в форме электрических сигналов, находящихся на любых носителях (примечание 1 к ст. 272 УК РФ).

В рамках состава преступления, предусмотренного ст. 272 УК РФ, предмет ограничен только информацией, охраняемой законом. При этом в Постановлении Пленума Верховного Суда РФ от 15.12.2022 № 37 представлено более широкое толкование данного понятия, поскольку, помимо какого-либо закона, закрепляющего особую охрану определенной информации, сам обладатель информации может установить средства ее защиты.

Таким образом, учитывая обязательность доказывания предмета преступления, при квалификации деяния по ст. 272 УК РФ правоприменительным органам следует отражать следующую информацию:

1) наличие сведений и их носитель;

2) охраняемость информации либо в соответствии с предписаниями закона, либо вследствие установления самим обладателем средств защиты от всеобщего доступа.

При этом анализ приговоров, размещенных на официальных сайтах судов субъектов РФ, показывает, что в большинстве случаев такие данные о предмете преступления отсутствуют.

К примеру, приговором Устиновского районного суда г. Ижевска Удмуртской Республики П. осужден по ч. 2 ст. 272 УК РФ. Судом указывается, что с целью последующей продажи информации о логине и пароле доступа к интернет-сайту путем подбора логина и пароля П. совершил неправомерный доступ ***к охраняемой законом компьютерной информации****, содержащейся в административной панели интернет-сайта*[1] *(выделено авт. —*

[1] Приговор № 1-256/2017 Устиновского районного суда г. Ижевска Удмуртской Республики. URL: https://sud-praktika.ru/precedent/546816.html (дата обращения: 08.05.2024). Аналогичные решения см.: https://sud-praktika.ru/precedent/467627.html; https://sud-praktika.ru/precedent/412143.html (дата обращения: 08.05.2024). Всего проанализировано 42 приговора.

О. Е.). Очевидно, что суды механически цитируют описание предмета преступления из диспозиции ст. 272 УК РФ, не устанавливая, о каком законе идет речь.

Полагаем, что подобная практика препятствует эффективному применению уголовно-правового запрета, а также может привести к отмене вынесенного решения. Правоприменительным органам необходимо уяснить предоставленную Верховным Судом РФ возможность не ограничивать действие ст. 272 УК РФ только информацией, охраняемой законом. В том случае, если обладатель информации сам установил средства ее защиты, она также может признаваться охраняемой. При этом в приговоре следует конкретизировать информацию, о каких средствах защиты идет речь. В случае же наличия ограничения со стороны какого-либо законодательного акта необходимо указать его наименование и иные реквизиты.

В качестве положительного опыта следует привести *приговор Ленинского районного суда г. Саратова по обвинению Д. в совершении преступления, предусмотренного ч. 3 ст. 272 УК РФ. В отдельном абзаце судом приводится детальная аргументация, позволяющая признать информацию охраняемой законом. «Компьютерная информация, хранящаяся в базе данных серверов ПАО "МТС", содержащая персональные данные абонентов, в соответствии с ч. 1 ст. 44 Конституции РФ, Федеральным законом от 27 июля 2006 г. № 149 «Об информации, информационных технологиях и о защите информации», ст. 1261, 1262 ГК РФ относится к охраняемой законом информации»*[1].

Кроме того, при вменении состава преступления, предусмотренного ст. 272 УК РФ, особое внимание необходимо уделить установлению самого деяния как обязательного признака объективной стороны, преступным последствиям и наличию между ними причинной связи. Наступление последствий из-за техниче-

[1] Приговор № 1-386/2017 Ленинского районного суда г. Саратова. URL: https://sud-praktika.ru/precedent/457282.html (дата обращения: 08.05.2024).

ских ошибок или неисправностей при отсутствии неправомерного доступа не может квалифицироваться по ст. 272 УК РФ.

В диспозиции ч. 1 ст. 272 УК РФ деяние описано как неправомерный доступ. Толкование признака «неправомерность» в принципе не вызывает вопросов и связывается с отсутствием полномочий, нарушением установленного порядка.

В свою очередь, понятие «доступ» в научной литературе трактуется неоднозначно. В частности, одни авторы чрезмерно ограничивают указанное понятие, полагая, что доступ есть использование лицом охраняемой информации[1]. Другие, наоборот, расширяют его содержание, включая в содержание наличие возможности получения информации[2].

Решение же вопроса о содержании понятия «доступ» имеет принципиально важное значение не только для квалификации деяния, но и для определения стадии совершения преступления (в частности, для констатации стадии покушения на преступление).

Анализ Постановления Пленума Верховного Суда РФ от 15.12.2022 № 37 по данному вопросу свидетельствует о том, что в разных частях указанного документа приводятся различные позиции. Так, в п. 5 постановления в большей степени отражается узкое толкование, поскольку закрепляется понятие доступа как получения или использования информации, исключая признанием доступа наличие только возможности.

В свою очередь, в п. 7 постановления, определяющего момент окончания преступления, указывается, что если лицо совершило все действия для доступа либо осуществило такой доступ, однако последствия не наступили, то содеянное квалифицируется как покушение на преступление.

Поскольку покушение предполагает начало выполнения действий, образующих объективную сторону конкретного состава

---

[1] См.: Филаненко А. Ю. Отграничения мошенничества в компьютерной информации от неправомерного доступа к компьютерной информации // Право и государство: теория и практика. 2013. № 1 (97). С. 59–62.

[2] См.: Сандаков А. Ц. Некоторые особенности квалификации неправомерного доступа к компьютерной информации // Инновации. Наука. Образование. 2021. № 28. С. 275–278.

преступления, то, исходя из совокупного толкования п. 5 и 7 постановления, доступ предполагает наличие возможности для неправомерного получения компьютерной информации либо непосредственно ее получение или использование.

Учитывая употребление законодателем конструкции материального состава преступления, стадия оконченного преступления при неправомерном доступе вменяется только при наступлении преступных последствий в виде уничтожения, блокирования, модификации или копирования компьютерной информации.

Стадия покушения на преступление будет иметь место не только при получении компьютерной информации либо уже ее использовании без наступления последствий, указанных в уголовном законе, но и при совершении действий, в результате которых виновный лишь приобретает возможность использования устройства, но не может довести умысел до конца. Например, лицо подбирает логин и пароль для входа в устройство, однако его действия прерываются и не приводят к получению информации по независящим обстоятельствам.

Систематизируя представленные выводы, полагаем, что возможна разработка следующих алгоритмов квалификации действий по неправомерному доступу в качестве неоконченного преступления:

1. Лицо не совершает действия по доступу, а только создает для этого условия — вменяется стадия приготовления к преступлению (при наличии тяжкого или особо тяжкого преступления).

2. Лицо начинает совершать действия по доступу и получает возможность ознакомиться с информацией, но не доводит действия до конца по независящим обстоятельствам — вменяется стадия покушения на преступление.

3. Лицо при доступе получает компьютерную информацию, но последствия не наступают — вменяется стадия покушения на преступление.

4. Лицо при доступе получает компьютерную информацию, что влечет ее копирование, модификацию, блокирование, уничтожение — вменяется стадия оконченного преступления.

В этой части следует признать неверным утверждение отдельных авторов о том, что «под уголовную ответственность не

попадают действия по незаконному ознакомлению с компьютерной информацией»[1]. Полагаем, что такие действия необходимо квалифицировать в качестве покушения на преступление.

Если неправомерный доступ к компьютерной информации выступает средством для совершения иного преступления (например, хищения), то содеянное квалифицируется по совокупности преступлений (п. 16 постановления от 15.12.2022 № 37).

Иная позиция изложена в апелляционном определении судебной коллегии по уголовным делам Московского городского суда, в соответствии с которым установлено, что Б. и А., имея умысел на тайное хищение денежных средств, путем незаконного получения информации с магнитных полос пластиковых платежных карт приискали устройство (комплект) для получения (перехвата) информации с магнитных полос пластиковых платежных карт и соответствующих пин-кодов и установили указанное оборудование на банкомат. При изъятии оборудования с информацией они были задержаны сотрудниками полиции. Суд указал, что квалификация по ч. 3 ст. 272 УК РФ является излишней, поскольку неправомерный доступ — это лишь способ совершения хищения[2].

Оценивая приведенное решение, полагаем, что в этой ситуации имеет место совокупность преступлений, предусмотренных ч. 3 ст. 30, п. «а» ч. 3 ст. 158, ч. 3 ст. 272 УК РФ. При этом неправомерный доступ образует оконченное преступление, поскольку произошло копирование информации.

Совокупность преступлений будет отсутствовать только в тех случаях, когда лицо осуществляет неправомерный доступ из корыстных побуждений, стремясь получить материальную выгоду или исключить затраты, но при этом хищения не совершает

[1] Демин Д. В. Проблемы квалификации неправомерного доступа к компьютерной информации // E-Scio. 2022. № 8 (71). С. 301–305.

[2] Дело №10-1144/14. URL: https://www.mos-gorsud.ru (дата обращения: 08.05.2024).

(например, неправомерный доступ осуществляется, чтобы скопировать информацию и продать ее третьим лицам).

Таким образом, при квалификации неправомерного доступа к компьютерной информации правоприменительным органам особое внимание необходимо уделить установлению: предмета преступления — охраняемой законом компьютерной информации путем указания того нормативного правового акта, в соответствии с которым доступ был ограничен, либо описания мер, предпринятых обладателем информации для ее сохранности; деяния в виде неправомерного доступа, означающего не только получение и использование компьютерной информации, но и возможность совершения таких действий; преступных последствий в виде копирования, модификации, блокирования, уничтожения информации.

В качестве предмета преступления, предусмотренного ст. 273 УК РФ, выступают компьютерная программа или иная компьютерная информация. Уяснение данного понятийного аппарата для правоприменителя представляется весьма затруднительным, поскольку предполагает освоение технических дефиниций.

При этом если понятие компьютерной программы закреплено на законодательном уровне (ст. 1261 ГК РФ) и представляет собой совокупность данных и команд, включая подготовительные материалы и порождаемые ею аудиовизуальные отображения, то понятие иной компьютерной информации приводится в п. 8 ППВС РФ от 15.12.2022 № 37 путем остаточного принципа, т. е. это любые сведения, которые в совокупности не представляют собой компьютерную программу (например, ключи доступа, элементы кодов и др.).

Обязательным признаком предмета преступления является его вредоносность, которая определяется возможностью несанкционированно уничтожать, блокировать, модифицировать, копировать компьютерную информацию или нейтрализовать средства защиты компьютерной информации.

В рамках уголовного дела вредоносность должна быть установлена с помощью эксперта и/или специалиста.

Например, «*согласно заключению специалиста… предоставленный на исследование образец файла… обладает функциями несанкционированного уничтожения, блокирования, модификации и копирования компьютерной информации*» или «*согласно заключению эксперта… файлы детектируются как вредоносные*»[1].

Некоторые правоприменители в формулировке обвинения перечисляют все признаки предмета преступления, изложенные в диспозиции статьи, даже если эксперт и/или специалист в результате его изучения приходят к другому выводу. Полагаем, что такая позиция является неверной. В каждом случае совершения преступления, предусмотренного ст. 273 УК РФ, в материалах обвинения необходимо отражать только такие вредоносные признаки предмета, которые он, исходя их своих свойств, содержит.

Так, по приговору Автозаводского районного суда г. Тольятти Самарской области действия Д.Я.ИА. судом были квалифицированы по ч. 2 ст. 273 УК РФ как умышленное использование компьютерной программы, заведомо предназначенной для несанкционированного уничтожения, блокирования и модификации компьютерной информации, совершенное с использованием своего служебного положения, из корыстной заинтересованности. Однако судебная коллегия Шестого кассационного суда общей юрисдикции, основываясь на установленных фактических обстоятельствах дела и заключении эксперта, указала, что признак программы «заведомо предназначенной для несанкционированного уничтожения компьютерной информации» вменен необоснованно и подлежит исключению из обвинения[2].

[1] Апелляционное постановление Верховного суда Республики Коми от 4 февраля 2022 г. № 22-277/2022 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Определение Шестого кассационного суда общей юрисдикции от 12 января 2022 г. № 77-326/2022 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

Ответственность по ст. 273 УК РФ наступает, если преступник создает, распространяет или использует вышеизложенный предмет преступления.

Отметим, что создание как признак объективной стороны данного состава преступления возможно толковать в двух аспектах: создание компьютерной программы либо создание иной компьютерной информации.

К созданию компьютерной программы необходимо причислять разработку новой (ранее не существовавшей) вредоносной программы (к примеру, могут включаться такие действия, как: написание исходного текста/кода; проверка работы этой программы (исполняемый/объектный код), выявление и исправление ошибок); а также внесение изменений в существующую вредоносную программу либо в ранее невредоносную программу. При этом момент окончания в каждой разновидности имеет определенные особенности. Так, создание новой (ранее не существовавшей) программы окончено с момента, когда она способна исполнять заданное предназначение (запускаться). Внесение изменений в существующую вредоносную программу оканчивается появлением иной компьютерной программы с другими (например, с расширенными или измененными и т. д.) вредоносными функциями, которые она способна исполнять.

Так, Г. вносил изменения в код программы @BEST_SCAM_BOT и их компоненты для корректной работы…, а также внедрял в программный код изменения для расширения функционала и оптимизации взаимодействия с пользователями, создавая таким образом новые экземпляры данных программ… Согласно заключениям эксперта… компьютерные программы avito_skam_bot и @BEST_SCAM_BOT представляют собой компьютерные программы…, предназначенные для несанкционированного копирования компьютерной информации, …а также модификации компьютерной информации…[1]

[1] Приговор Нижегородского районного суда Нижнего Новгорода от 12 августа 2022 г. по делу № 1-165/2022 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

Также преступным становится внесение изменений в программу, не являющуюся вредоносной, с момента, когда в нее добавляется вредоносный фрагмент кода и, следовательно, она приобретает возможность несанкционированного уничтожения, блокирования, модификации, копирования информации или нейтрализации средств защиты.

К созданию иной компьютерной информации следует относить деятельность по разработке подготовительных материалов вредоносной компьютерной программы (например, написание исходного текста/кода), а также других сведений (данных или команд), если не было еще завершено создание такой программы.

Поскольку лицо создает компьютерную программу или иную информацию, обладающие вредоносными способностями, то чаще всего у него наличествуют намерения в будущем ее применить. В этой связи в правоприменительной практике по ст. 273 УК РФ в подавляющем большинстве случаев фиксируется совокупность преступных действий, квалифицируемых как создание и использование.

> *Например, Р. совершил разработку вредоносного программного обеспечения, имитирующего сайт платежного сервиса, и использовал ее на сервере поставщика хостинг-услуг, тем самым копируя логины и пароли пользователей платёжной системы*[1]. При этом совокупности преступлений в действиях такого лица нет, здесь необходима квалификация по одному факту ст. 273 УК РФ, поскольку данный состав сложный с альтернативными действиями.

Под использованием предмета исследуемого преступления необходимо понимать его применение, в результате которого происходит умышленное уничтожение, блокирование, модификация, копирование компьютерной информации или нейтрализа-

[1] Приговор Приволжского районного суда г. Казани Республики Татарстан от 9 ноября 2018 г. по делу № 1-588/2018. URL: http:// www.sudact.ru (дата обращения: 08.05.2024).

ция средств ее защиты[1]. Стоит отметить, что использование вредоносной программы или информации может осуществляться лицом как на личном компьютерном устройстве (ЭВМ) (*К. приобрел игровую консоль и для получения возможности воспроизведения на ней нелицензионных программных продуктов использовал установленные компьютерные программы, которые предназначены для несанкционированного блокирования компьютерной информации и нейтрализации средств защиты компьютерной информации*[2]), так и на устройстве, принадлежащем другому лицу (*К. скачал из интернета файлы компьютерной программы, заведомо предназначенной для нейтрализации средств защиты компьютерной информации, на свой ноутбук, затем, запустив эту программу в интернете, осуществил компьютерное воздействие на различные IP-адреса типа компьютерной атаки)*[3].

Таким образом, независимо от того, совершается ли разработка и использование одновременно либо имеет место только одно из этих действий, квалификация осуществляется только по ст. 273 УК РФ.

В том случае, если лицо использует вредоносную компьютерную программу для совершения иного преступления (например, предусмотренного ст. 137, 138, 159[6] УК РФ и т. п.), то требуется квалификация преступлений по совокупности со ст. 273 УК РФ.

Согласно п. 11 ППВС РФ от 15.12.2022 № 37 под распространением вредоносной компьютерной программы или иной информации понимается предоставление доступа к ним конкрет-

---

[1] 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» [Электронный ресурс]: постановление Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37, п. 11. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Приговор Валуйского районного суда Белгородской области от 27 сентября 2021 г. по делу № 1-123/2021 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

[3] Приговор Павловского районного суда Воронежской области от 25 ноября 2020 г. по делу № 1-40/2020. URL: http:// www.sudact.ru (дата обращения: 08.05.2024).

ным лицам или неопределенному кругу лиц любым способом (например, продажа, рассылка, передача копии на электронном носителе либо с использованием сети Интернет, размещение на серверах, предназначенных для удаленного обмена файлами). При этом такая программа или информация может содержаться на любом носителе (устройстве)[1].

Например, С., разместив объявление о продаже спутникового приемника и смарт-карты, позволяющих несанкционированно просматривать телеканалы «Триколор» по нескольким подпискам, затем продал их, тем самым совершив распространение иной компьютерной информации, содержащейся на модифицированной смарт-карте, заведомо предназначенной для несанкционированной нейтрализации средств защиты компьютерной информации, из корыстной заинтересованности[2].

На практике неоднозначную оценку получают случаи установки (запуска) вредоносной компьютерной программы преступником на чужом компьютере. Одни суды квалифицируют эти действия как распространение компьютерной программы: *П., осуществляя индивидуальную предпринимательскую деятельность по ремонту компьютеров и периферийного компьютерного оборудования, а также по копированию записанных носителей информации на его компьютерной технике, на просьбу обратившегося клиента о возможности загрузить какие-либо программы для черчения установил вредоносную компьютерную программу на его компьютер. Суд установил, что доказательств наличия у П. корыстной заинтересованности в распространении компьютерных программ не имеется, и признал его виновным по ч. 1 ст. 273 УК РФ в распространении компьютер-*

[1] Уголовное право Российской Федерации. Особенная часть: учебник. Изд. второе, испр. и доп. / под ред. Л. В. Иногамовой-Хегай, А. И. Рарога, А. И. Чучаева. М.: Юридическая фирма «Контакт»: ИНФРА-М, 2009. С. 558.

[2] Приговор Заводского районного суда г. Орла от 11 ноября 2021 г. по делу № 1-323/2021 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

ных программ, заведомо предназначенных для несанкционированной нейтрализации средств защиты компьютерной информации[1]. Другие правоприменители оценивают подобное деяние как использование программы: *И., находясь у себя дома, скачал вредоносные компьютерные программы, а затем за 500 рублей установил их на компьютер в помещении офиса, расположенного в торговом центре. Суд вменил ч. 3 ст. 30, ч. 2 ст. 273 УК РФ — покушение на использование компьютерных программ, заведомо предназначенных для нейтрализации средств защиты компьютерной информации, совершенное из корыстной заинтересованности*[2].

Полагаем, что вышеизложенные случаи, связанные с установкой (запуском) компьютерной программы на чужом компьютере, направлены на ее введение в хозяйственный оборот[3] (применение вредоносных свойств такой программы по назначению), а не на сбыт или иное предоставление доступа к ней. В такой ситуации ответственность для виновного должна наступать за использование программы.

Если действия виновного лица содержат в себе элементы как распространения, так и использования вредоносной компьютерной программы или иной вредоносной компьютерной информации, оба эти действия должны быть указаны в приговоре[4].

Для правильной квалификации действий лица по ст. 273 УК РФ требуется установление признака заведомости по отношению к характеристике предмета преступления. Исследование судеб-

---

[1] Приговор Фокинского районного суда г. Брянска от 14 сентября 2022 г. по делу № 1-145/2022. URL: http:// www.sudact.ru (дата обращения: 08.05.2024).

[2] Приговор Тербунского районного суда Липецкой области от 17 мая 2018 г. по делу № 1-17/2018. URL: http:// www.sudact.ru (дата обращения: 08.05.2024).

[3] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации (утв. Генпрокуратурой России) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

[4] 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» [Электронный ресурс]: постановление Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37, п. 11. Доступ из справ.-правовой системы «КонсультантПлюс».

ной практики показывает, что в материалах дела заведомость доказывается уровнем образования преступника, позволяющего ему осознавать вредоносное предназначение программы или иной информации (например, *К. с учетом полученного технического образования осознавал, что внесение им изменений в системное программное обеспечение игровых приставок приведет к возможности воспроизведения на игровых консолях нелицензионных программных продуктов*[1], *или …у Б., имеющего высшее образование по специальности «Информатика и вычислительная техника», возник умысел, направленный на использование компьютерных программ, заведомо предназначенных для несанкционированной нейтрализации средств защиты компьютерной информации…*[2]), либо наличием специальных знаний и/или навыков (*…К., обладая достаточными познаниями в области компьютерной техники и навыками работы в сети Интернет…*[3], *…П., обладающего достаточными знаниями в области информационных технологий…*)[4].

Сложившуюся судебную практику следует признать положительной и рекомендовать работникам правоохранительных органов отражать характеристики образования, специальных знаний и/или навыков в материалах дела при установлении заведомости.

Кроме того, Пленум Верховного Суда РФ в п. 11 постановления от 15.12.2022 № 37 обязывает правоприменителей при привлечении лица к ответственности по ст. 273 УК РФ устанавливать еще два момента: во-первых, то, с какой целью лицо совершило преступление, во-вторых, наступили ли от него последствия в виде несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или

---

[1] Постановление Первого кассационного суда общей юрисдикции от 2 ноября 2022 г. № 77-5125/2022 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Постановление Заводского районного суда г. Кемерово от 27 мая 2020 г. по делу № 1-889/2019. URL: http:// www.sudact.ru (дата обращения: 08.05.2024).

[3] Приговор Ленинского районного суда г. Оренбурга от 23 июля 2020 г. по делу № 1-538/2020. URL: http:// www.sudact.ru (дата обращения: 08.05.2024).

[4] Приговор Вологодского городского суда Вологодской области от 24 сентября 2020 г. по делу № 1-1094/2020. URL: http:// www.sudact.ru (дата обращения: 08.05.2024).

нейтрализации средств ее защиты. Так, если лицо на принадлежащем ему компьютере либо с согласия собственника компьютерного устройства совершит, например, использование вредоносной программы, но с правомерными целями (образовательные или тестирование компьютерных систем для проверки уязвимости средств защиты компьютерной информации, к которым у данного лица имеется правомерный доступ), то состав преступления в его действиях будет отсутствовать.

Представляется, что причинами ограниченного количества судебно-следственной практики по ст. 274 УК РФ являются латентность данной формы преступных деяний[1], а также проблемы толкования признаков рассматриваемого состава. Кроме того, возникают сложности в доказывании нарушения правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, нарушения правил доступа к информационно-телекоммуникационным сетям, а также причиненного преступлением ущерба, который согласно примечанию к ст. 272 УК РФ должен превышать один миллион рублей.

Не останавливаясь подробно на предмете преступления, предусмотренного ст. 274 УК РФ, поскольку понятия средств хранения, обработки или передачи компьютерной информации, информационно-телекоммуникационных сетей и оконечного оборудования регламентированы действующим законодательством[2], считаем необходимым перейти к рассмотрению особенностей объективной стороны и субъекта данного преступного посягательства.

---

[1] Евдокимов К. Н. К вопросу о совершенствовании объективной стороны состава преступления при нарушении правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей // Российская юстиция. 2019. № 3. С. 10–13.

[2] См., например: Об информации, информационных технологиях и защите информации [Электронный ресурс]: федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ (ред. от 12.12.2023). Доступ из справ.-правовой системы «КонсультантПлюс»; О связи [Электронный ресурс]: федеральный закон Российской Федерации от 7 июля 2003 г. № 126-ФЗ (ред. от 06.04.2024). Доступ из справ.-правовой системы «КонсультантПлюс».

В силу бланкетного характера диспозиции ч. 1 ст. 274 УК РФ и указания в судебных разъяснениях лишь на необходимость установления конкретных правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, информационно-телекоммуникационных сетей, оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям и факта возложения на виновного обязанности их соблюдать[1] для правильной квалификации действий виновного следует выяснить, чем данные правила регламентированы.

Учитывая широкий круг средств хранения, обработки или передачи компьютерной информации (ЭВМ, персональные компьютеры, ноутбуки, смартфоны, банкоматы, контрольно-кассовая техника, карты памяти, USB-флеш-накопители, платежные карты, дискеты, диски и т. п., т. е. любые предметы, на которых может содержаться компьютерная информация), разработать какие-либо общие правила их эксплуатации достаточно сложно. Представляется целесообразным привести в пример лишь некоторые нормативные правовые акты, устанавливающие отдельные интересующие нас правила на государственном уровне. К ним следует отнести федеральный закон «О применении контрольно-кассовой техники при осуществлении расчетов в Российской Федерации»[2], в котором раскрывается понятие контрольно-кассовой техники, являющейся предметом данного преступления, закрепляются правила, особенности, порядок и условия ее применения; положение Центрального банка РФ «Об эмиссии платёжных карт и об операциях, совершаемых с их

[1] 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» [Электронный ресурс]: постановление Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37, п. 12. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] О применении контрольно-кассовой техники при осуществлении расчётов в Российской Федерации [Электронный ресурс]: федеральный закон Российской Федерации от 22 мая 2003 г. № 54-ФЗ (ред. от 29.12.2022). Доступ из справ.-правовой системы «КонсультантПлюс».

использованием»[1], устанавливающее порядок совершения операций с использованием платежных карт; отдельные технические стандарты, регламентирующие общие технические требования, правила приемки, методы испытаний, маркировку, упаковку, транспортирование и хранение ПЭВМ[2]. Существуют также рекомендации по классифицированию мест установки банкоматов и платежных терминалов, их оснащению защитным оборудованием и специальным программным обеспечением, системами видеонаблюдения и т. п.[3] и другие нормативные правовые акты.

Кроме того, анализ судебной практики позволяет прийти к выводу о том, что правила эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, за нарушение которых виновный несет уголовную ответственность, могут устанавливаться инструкциями или иными локальными актами организации. Согласно разъяснениям высшего судебного органа России, они должны быть приняты в развитие законов и подзаконных актов, не должны им противоречить и изменять их содержание[4].

---

[1] Об эмиссии платёжных карт и об операциях, совершаемых с их использованием [Электронный ресурс]: положение Центрального Банка Российской Федерации от 24 декабря 2004 г. № 266-П (ред. от 28.09.2020). Доступ из справ.-правовой системы «КонсультантПлюс».

[2] См., например: ГОСТ 27201-87 Машины вычислительные электронные персональные. Типы, основные параметры, общие технические требования; ГОСТ 21552-84 Средства вычислительной техники. Общие технические требования, приемка, методы испытаний, маркировка, упаковка, транспортирование и хранение и др.

[3] О рекомендациях по повышению уровня безопасности при использовании банкоматов и платежных терминалов [Электронный ресурс]: письмо Банка России от 1 марта 2013 г. № 34-Т. Доступ из справ.-правовой системы «КонсультантПлюс».

[4] 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» [Электронный ресурс]: постановление Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37, п. 12. Доступ из справ.-правовой системы «КонсультантПлюс».

Так, *Р., являясь начальником научно-исследовательской группы научно-исследовательского отделения вычислительной математики института теоретической и математической физики (далее — ИТМФ ФГУП «РФЯЦ-ВНИИЭФ» или ИТМФ), был признан виновным в совершении преступления, предусмотренного ч. 1 ст. 274 УК РФ.*

...В период времени с 1 июля 2017 г. по 5 февраля 2018 г. с целью создания условий для использования вычислительных ресурсов (мощностей) собранной фермы при вычислении (майнинге) криптовалюты Р. совместно с Л. с использованием своего служебного положения, действуя в нарушение: пункта 2 Инструкции № 8/26606-дсп, пункта 5 Инструкции № 195-96/111145-дсп, пункта 7 Аттестата СВС, положений указа № 351, пункта 5.5 СТР-97, положений СТ2003, пунктов 5, 6 Инструкции № 20209, пункта 1 приказа директора № 195/4328-П-дсп, соединили подключенное СЛВС и АСЗИ ЗЛВС ИТМФ вычислительное оборудование ОТКС «Интернет» посредством GSM-модема, т. е. посредством использования переносного устройства для организации беспроводного доступа к сети Интернет на территории режимной площадки, а также установили и запустили на указанном оборудовании нештатное программное обеспечение, не разрешенное к применению комиссией, созданной на основании приказа от 20.06.2014 № 195/1783-П, предназначенное для вычисления криптовалюты, чем нарушили действующие во ФГУП «РФЯЦ-ВНИИЭФ» правила эксплуатации средств хранения, обработки и передачи охраняемой компьютерной информации.

Из заключения компьютерной судебной экспертизы № 214 от 15 марта 2019 г. следует, что в результате действий Р. и Л. по организации канала передачи данных между узлами вычислительного поля сегмента САУ-300 АСЗИ ЗЛВС и ОТКС «Интернет», необходимого для выполнения расчетов (майнинга) криптовалюты, а именно физического соединения АСЗИ ЗЛВС и СЛВС, подключения к СЛВС постороннего компьютера, имеющего соединение с ОТКС «Интернет» посредством 3G-модема, был осу-

ществлен доступ к ресурсам ЗЛВС, т. е. к охраняемой законом компьютерной информации, составляющей государственную тайну, которая хранится, обрабатывается и передается в указанной защищенной сети. Указанные действия Р. и Л. повлекли модификацию компьютерной информации, которая выразилась в изменении служебной информации, используемой активным сетевым оборудованием АСЗИ ЗЛВС и СЛВС, а также модификацию компьютерной информации, которая выразилась в генерации сетевого трафика.

Согласно письму ИТМФ от 15.05.2019 № 195-96/22729-дсп вышеуказанные действия Р. и Л. по нарушению установленных в ИТМФ правил эксплуатации средств хранения, обработки и передачи охраняемой компьютерной информации в соответствии с п. 4.27 «Типовой инструкции по защите информации в автоматизированных системах предприятий и организаций Федерального агентства по атомной энергии», введенной во ВНИИЭФ приказом от 06.09.2006 № 960/ВР дсп, а также п. 8 «Аттестата соответствия объекта информатизации "Автоматическая система в защищённом исполнении «Закрытая локальная вычислительная сеть ИТМФ»" требованиям по безопасности информации» повлекли необходимость в проведении сотрудниками ИТМФ внеплановых дополнительных работ (проверок, инвентаризации, иных организационных мер) по восстановлению надлежащего уровня защищенности МП-1Р/300САУ, стоимость которых составила 1 087 448 (один миллион восемьдесят семь тысяч четыреста сорок восемь) рублей 19 копеек[1].

Следующей особенностью состава преступления, предусмотренного ст. 274 УК РФ, является уникальность его конструкции, заключающаяся в том, что для привлечения виновного к уголовной ответственности требуется обязательное наступление двух

[1] Архив Саровского городского суда Нижегородской области. Дело № 1-167 за 2019 г. URL: http://sarovsky.nnov.sudrf.ru/ (дата обращения: 08.05.2024).

абсолютно разных последствий — нематериального вреда (уничтожение, блокирование, модификация либо копирование компьютерной информации) и материального в виде имущественного вреда, имеющего денежное выражение (ущерба свыше одного миллиона рублей).

Анализ судебной практики позволяет прийти к выводу о том, что итоговая сумма причиненного преступлением ущерба включает в себя не только фактические издержки, понесенные потерпевшей стороной в результате преступных действий, но и сопутствующие расходы, обуславливаемые необходимостью восстановления данных или доступа к ним, замены программных продуктов, простоем, упущенной выгодой и другими факторами[1]. Основополагающим при этом является установление факта причинения именно крупного ущерба.

Например, по делу А. *ущерб органами предварительного расследования был установлен исходя из действий, направленных на ликвидацию последствий для самой организации, выполненных уже после преступления. А именно: восстановление доступа к базе данных после смены всех паролей сотрудников, проведение комплекса мероприятий, направленных на поиск лица, которое копировало информацию, средний простой сотрудников организации, покупка необходимого оборудования, введение дополнительных средств учета лиц, осуществляющих доступ к базе данных, оцененные в общую сумму 1 155 600 рублей. В то же время фактическая стоимость собственно скопированной компьютерной информации органами предварительного расследования не устанавливалась*[2].

[1] Малетина М. А., Диянов Н. М. Совершенствование уголовно-правовых мер противодействия преступлениям в сфере компьютерной информации // Вестник Барнаульского юридического института МВД России. 2022. № 1 (42). С. 178–180.

[2] Постановление Лефортовского районного суда г. Москвы от 29 сентября 2016 г. по делу № 1-277/2016. URL: https://advocate-service.ru/sud-praktika/ugolovnye-dela/prigovory-sudov-po-st.-274-uk-rf-narushenie-pravil-ekspluatatsii-sredstv-hranenija-obrabotki-ili-peredachi-kompjuternoj-informatsii-i-inform/prigovor-suda-po-ch.-1-st.-274-uk-rf--1-2772014--sudebnaja-praktika.html (дата обращения: 08.05.2024).

Несмотря на то что в диспозиции ст. 274 УК РФ указание на специальный субъект отсутствует, исходя из особенностей объективной стороны, заключающейся в нарушении определенных правил, следует вывод о том, что лицо подлежит уголовной ответственности только при наличии у него установленной должностными инструкциями обязанности соблюдать и руководствоваться определенными правилами в силу занимаемого служебного положения.

Именно поэтому в п. 12 постановления Пленума Верховного Суда РФ от 15.12.2022 № 37 указывается на необходимость доведения до сведения лица обязанности соблюдать установленные правила обращения с компьютерной информацией.

Анализ судебной практики показывает, что обозначенное требование не соблюдается правоприменительными органами, поскольку в приговорах отражается лишь факт занятия той или иной должности, без конкретизации наличия ознакомления виновного с правилами, за нарушение которых он привлекается к уголовной ответственности[1].

Таким образом, при квалификации деяния по ст. 274 УК РФ правоприменительным органам необходимо особое внимание уделять установлению следующих обстоятельств: наличие специального порядка обращения с компьютерной информацией, закрепленного в нормативных правовых актах РФ, субъектов РФ либо локальных актах организации; наличие у виновного лица обязанностей соблюдения специальных правил и его ознакомления с ними; наступление преступных последствий, с которыми законодатель связывает момент окончания преступления и возможность привлечения к уголовной ответственности.

[1] Архив Саровского городского суда Нижегородской области. Дело № 1-167 за 2019 г. URL: http://sarovsky.nnov.sudrf.ru/ (дата обращения: 08.05.2024).

2.4. Уголовно-правовое предупреждение отдельных преступлений против здоровья населения и общественной нравственности, совершаемых с использованием информационно-телекоммуникационных технологий

Анализ особенностей современной преступности показывает, что использование цифровых средств выступает характерным способом незаконного сбыта наркотических средств, психотропных веществ, аналогов, растений. Именно поэтому справедливым представляется утверждение о том, что большая часть таких преступлений трансформировалась в разряд бесконтактных.

Несмотря на то что в постановлении Пленума Верховного Суда РФ от 15 июня 2006 г. № 14 закрепляется общее понятие сбыта как возмездной или безвозмездной реализации наркотических средств, совершение деяния бесконтактно при помощи различных мессенджеров, подключенных к сети Интернет, создает значительные сложности в квалификации.

Одной из первых таких проблем выступает отграничение единичного продолжаемого сбыта от совокупности преступлений.

В судебной практике сформировалась единая позиция, заключающаяся в том, что каждый факт закладки образует самостоятельное преступление.

Например, С. было вменено два эпизода сбыта наркотических средств с использованием информационно-телекоммуникационных сетей (Интернет), группой лиц по предварительному сговору, в крупном размере. При этом в приговоре указано, что С. получил для осуществления закладок партию синтетических наркотических средств. 11 июня 2021 г. он сделал закладку в тайнике, адрес которого сообщил неустановленному следствием лицу.[1]

[1] Дело № 1-346/21. URL: https://sud-praktika.ru/precedent/422334.html (дата обращения: 08.05.2024).

В определении суда кассационной инстанции Верховного Суда РФ от 26.07.2016 № 5-УД16-61, вынесенном в связи с подачей осужденным О. кассационной жалобы на необоснованную квалификацию его действий в качестве самостоятельных преступлений, указано, что осужденный покушался на сбыт наркотических средств двум разным лицам. Из показаний осужденного не усматривается, что изначально была договоренность на приобретение всего объема наркотических средств[1].

Решение вопроса квалификации действий лица как продолжаемого преступления либо совокупности следует из самого понятия продолжаемого преступления как деяния, состоящего из тождественных действий, совершаемых с единым умыслом.

Исходя из этого, возможно выделить несколько типовых ситуаций, свидетельствующих о наличии продолжаемого преступления либо совокупности:

1. Сбыт осуществляется в несколько приемов, но одному лицу, при этом лица заранее договорились о реализации всего объема — продолжаемое преступление.

2. Сбыт осуществляется разными лицами, но сговор был сразу на реализацию всего объема наркотических средств — продолжаемое преступление.

3. Сбыт производился с неопределенным умыслом, ситуативно — совокупность преступлений.

Второй проблемой является понимание терминов «электронная сеть», «информационно-телекоммуникационная сеть».

В большинстве научных источников данные понятия рассматриваются как синонимы, вследствие чего авторами делается вывод об избыточности их разделения[2].

---

[1] Определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации № 5-УД16-61 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Винокуров В. Н., Агафонов А. В. Особенности квалификации сбыта наркотических средств с использованием электронных или информационно-телекоммуникационных сетей (включая сеть Интернет) // Уголовное право. 2023. № 1. С. 3–12.

При этом судебная практика исходит из того, что средства связи (например, сотовый телефон) нельзя отнести к использованию информационно-телекоммуникационных сетей[1].

В соответствии с Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» информационно-телекоммуникационная сеть — это технологическая система, предназначенная для того, чтобы передавать по линиям связи информацию, доступ к которой исполняется при помощи средств вычислительной техники. Исходя из данного понятия, применение при сбыте даже сотовой связи дает основание для вменения п. «б» ч. 2 ст. 228[1] УК РФ.

Анализируя судебную практику, можно выделить несколько типовых ситуаций применения п. «б» ч. 2 ст. 228[1] УК РФ:

– когда расчет за приобретение наркотических средств осуществляется при помощи электронных средств платежа;

– сбыт осуществляется в сети Интернет на различных сайтах;

– сбыт осуществляется при помощи телеграм-каналов иных социальных сетей.

Третья группа проблем связана с определением видов соучастников преступления. Правильное решение данного вопроса влияет не только на квалификацию преступления (действия исполнителя не требуют ссылки на ст. 33 УК РФ, в отличие от действий иных соучастников (ст. 34 УК РФ)).

В осуществлении бесконтактного сбыта участвуют большое количество субъектов, роли которых существенным образом различаются. В частности, исследователями в области криминологической науки выделяются: координаторы (которые осуществляют общее руководство процессом сбыта), закладчики (лица, которые делают закладку в установленном месте), диспетчеры (лица, производящие переписку с приобретателем), касси-

[1] Постановление президиума Челябинского областного суда от 11 июля 2018 г. по делу № 44у-89/2018 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

ры (функция которых заключается в обналичивании денежных средств, полученных от сбыта) и т. д.[1]

При определении роли лиц, участвующих в процессе совершения преступления, в первую очередь следует руководствоваться понятием сбыта, поскольку характеристика действий, образующих объективную сторону преступления, напрямую влияет на признание лица исполнителем (соисполнителем).

В действующем постановлении Пленума Верховного Суда РФ от 15 июня 2006 г. № 14 представлен новый подход к пониманию сбыта (ранее использовалось узкое значение сбыта как передачи), а именно как деятельности, направленной на реализацию наркотических средств. Учитывая, что такая деятельность включает в себя различные проявления в виде создания сайтов по продаже наркотиков, координацию, общение с будущими закладчиками и т. д., любое ее проявление можно признать выполнением объективной стороны. Соответственно, действия таких лиц следует квалифицировать в качестве соисполнительства.

Если же совершенные лицом действия выходят за рамки реализации, к примеру обналичивание полученных денежных средств осуществляется уже после сбыта, то такое деяние образует пособничество и квалифицируется со ссылкой на ч. 5 ст. 33 УК РФ.

При этом в случае, когда лицо передает приобретателю наркотические средства по просьбе (поручению) другого лица, которому они принадлежат, его действия следует квалифицировать как соисполнительство в незаконном сбыте.

Интерес представляет установление момента окончания бесконтактного сбыта. В соответствии с п. 13 постановления Пленума Верховного Суда РФ от 15 июня 2006 г. № 14 передача лицом реализуемых средств, веществ, растений приобретателю может быть осуществлена любыми способами, в т. ч. непосредственно, путем сообщения о месте их хранения приобретателю,

[1] Сретенцев А. Н. Особенности «бесконтактного» способа сбыта наркотических средств или психотропных веществ на современном этапе с использованием сети Интернет // Уголовно-процессуальные и криминалистические проблемы борьбы с преступностью: сборник материалов, Орел, 25 мая 2018 г. Орел: Орловский юридический институт МВД России имени В. В. Лукьянова, 2018. С. 194–200.

проведения закладки в обусловленном с ним месте, введения инъекции. То есть фактически для признания сбыта оконченным не требуется, чтобы покупатель уже получил наркотические средства. Достаточно совершение всех активных действий самим сбытчиком.

Существенные проблемы квалификации присущи незаконному обороту порнографических материалов или предметов, совершенному с использованием информационно-телекоммуникационных сетей, в т. ч. сети Интернет.

Термин «оборот порнографических материалов или предметов, совершенный с использованием информационно-телекоммуникационных сетей, в том числе сети "Интернет"», встречается в УК РФ в двух статьях — 242 и 242.1.

Соотношение названия ст. 242 УК РФ и ее диспозиции позволяет сделать вывод, что к обороту порнографических материалов и предметов, совершенному с использованием информационно-телекоммуникационных сетей, в т. ч. сети Интернет, следует причислять их распространение, публичную демонстрацию либо рекламирование; соответственно, в ст. 242.1 УК РФ — приобретение, распространение, публичную демонстрацию, рекламирование.

При этом, не вдаваясь в суть понятий порнографических материалов или предметов, а также материалов или предметов с порнографическими изображениями несовершеннолетних, отметим, что в сети Интернет возможно совершить в отношении таких материалов распространение, приобретение, демонстрацию и рекламирование, а в отношении порнографического предмета — только рекламирование. Вывод о том, может ли материал или предмет быть признан предметом преступлений, предусмотренных ст. 242 или 242.1 УК РФ, должен быть сделан только на основании проведенной судебной экспертизы.

Для того чтобы привлечь лицо по п. «б» ч. 3 ст. 242 УК РФ или п. «г» ч. 2 ст. 242.1 УК РФ, в материалах дела необходимо расписать, в чем конкретно проявилось каждое из перечисленных действий объективной стороны.

Подчеркнем, что такие деяния, как распространение, публичная демонстрация, рекламирование, применительно к ст. 242,

242.1 УК РФ получили толкование только в конце 2022 г. в связи с принятием ППВС РФ от 15.12.2022 № 37[1]. До этого момента судебная практика складывалась неоднозначно.

Так, касаясь дефиниции распространения порнографических материалов, отметим, что суды основывались на п. 9 ст. 2 ФЗ 2006 г. № 149-ФЗ, согласно которому распространение информации — действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц[2]. Таким образом, способ распространения представлялся слишком широким, что привносило дополнительные трудности в правоприменении.

В частности, одни суды, следуя положению ст. 2 ФЗ № 149-ФЗ, причисляли к распространению материала его передачу любым способом, например таким, как продажа. *Ж., используя сетевой псевдоним, разместил в сети Интернет со своего компьютерного устройства объявление о продаже материалов с порнографическими изображениями несовершеннолетних. Данные действия в результате ОРМ были выявлены сотрудниками правоохранительных органов, которые после переписки с Ж. перевели на его электронный кошелек денежную сумму, а взамен получили*

[1] О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»: постановление Пленума Верховного Суда Российской Федерации от 15.12.2022 № 37 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Об информации, информационных технологиях и о защите информации [Электронный ресурс]: федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс»; Обобщение судебной практики по уголовным делам о преступлениях, совершенных с использованием информационно-телекоммуникационных сетей, включая сеть «Интернет». URL: http://oblsud.cht.sudrf.ru/modules.php?name=docum_sud&id=195 (дата обращения: 08.05.2024); Кассационное определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 08.12.2022 № 1-УДП22-10-К3 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

файлы и ссылки для скачивания нескольких файлов порнографического характера[1].

Другие суды четко не отграничивали между собой деяния объективной стороны в виде распространения порнографических материалов и их публичной демонстрации, и зачастую публичная демонстрация не выделялась как отдельное альтернативное преступное деяние, а поглощалась незаконным распространением.

Так, Н. в течение двух месяцев в социальной сети «ВКонтакте» на личной странице размещал к всеобщему просмотру и скачиванию видеофайл и фотофайлы, содержащие информацию порнографического характера, которые были неоднократно просмотрены другими пользователями. Суд, вынося обвинительный приговор по п. «б» ч. 3 ст. 242 УК РФ за единое продолжаемое преступление, пояснил, что: «…Публично демонстрируя характер содержания.., хранящегося на его странице.., предоставил возможность любому желающему зарегистрированному пользователю сайта "ВКонтакте" скопировать и приобрести… Таким образом, Н. незаконно распространил порнографические материалы…»[2].

На сегодняшний день ППВС РФ от 15.12.2022 № 37 в п. 22 разграничивает между собой понятия распространения и демонстрации материалов порнографического характера. Так, распространение — это предоставление возможности их использования такими способами, как: 1) направление в личном сообщении конкретному лицу; 2) рассылка; 3) размещение на личных стра-

[1] Приговор Дзержинского районного суда г. Новосибирска от 1 февраля 2017 г. Д. № 1-72/2017. URL: https://sud-praktika.ru/precedent/546755.html (дата обращения: 08.05.2024).

[2] Приговор Октябрьского районного суда г. Пензы от 10 января 2020 г. Д. № 1-11/2020 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

ницах и на страницах групп пользователей ссылки для загрузки (скачивания) файлов.

Возникает вопрос, для привлечения виновного лица к ответственности по ст. 242, 242.1 УК РФ достаточно самого факта распространения материалов или необходимо, чтобы иное конкретное лицо с ними ознакомилось? Материалы правоприменительной практики свидетельствуют, что чаще всего лиц осуждают за сам факт распространения порнографических материалов даже без показаний свидетелей, ознакомившихся с ними.

Так, Судебная коллегия Верховного Суда РФ одним из доводов отмены решения нижестоящих судов и отправки дела на новое рассмотрение в отношении Н. признала следующее: «…согласно диспозиции ст. 242.1 УК РФ инкриминируемое осужденному преступление не предполагает в качестве обязательного своего признака фактический просмотр кем-либо из посетителей его страницы с размещенным на ней порнографическим сайтом; достаточно уже того, что, размещая в социальной сети «ВКонтакте» такой сайт, осужденный исходил из того, что этот сайт может быть просмотрен неопределенным кругом лиц…»[1].

Подобный случай возможен, когда сотрудники правоохранительных органов для выявления факта незаконного оборота порнографических материалов используют специальную компьютерную программу, которая в сети Интернет обнаруживает наличие в IP-адресе, принадлежащем кому-либо, такого материала.

Возникают трудности с оценкой случаев, когда лицо, желая посмотреть видеофайл с информацией порнографического характера, скачивает его при помощи специальной компьютерной программы-файлообменника, установленной на его компьютерном устройстве, которая автоматически открывает доступ другим пользователям сети Интернет скачать его себе. В таком слу-

[1] Кассационное определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 22.03.2022 № 14-УДП22-1-К1 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

чае не ясно, наличествуют ли в действиях этого лица признаки распространения порнографических материалов или нет.

Исследование практики показало, что суды при рассмотрении дела устанавливают у лица знание об особенностях программы-файлообменника предоставлять возможность другим пользователям скачивать файлы, содержащие информацию порнографического характера. Однако в одном случае это признается как обстоятельство, не свидетельствующее об умысле лица на распространение таких материалов, а в другом случае дополнительно к этому назначается компьютерно-техническая экспертиза, которая может прийти к выводу, что лицо осуществляло целенаправленные действия по незаконному распространению материалов. В итоге суды принимают разные решения.

Так, одним из доводов отмены приговора и решений нижестоящих судов, которые квалифицировали действия Х. по ст. 242.1 УК РФ за приобретение, хранение в целях распространения и распространение материалов с порнографическими изображениями несовершеннолетних, за отсутствием в его действиях состава преступления, был следующий: *«…установив, что программа “StrongDC++”, являющаяся программой файлообменной сети “<...>”, позволяет пользователям сети “Интернет”, установившим на принадлежащих им компьютерах программу, работающую по принципу “<...>”, осуществлять скачивание и передачу файлов в свободном доступе, суд, не привел доказательств, свидетельствующих о том, что файлы с порнографическими изображениями, полученные в ходе оперативно-розыскных мероприятий, были распространены в результате прямого умысла Х., а не в результате особенностей работы программы, установленной на компьютере, которая автоматически передавала скачанные файлы. То обстоятельство, что Х. было известно о сохранении скачанных на компьютер файлов порнографического содержания и особенностях программы, позволяющей другим пользователям скачивать данные файлы, само по себе не свидетельствует о прямом умысле осужденного*

на их распространение, а при косвенном умысле, если виновное лицо не желает, а только допускает возможность наступления общественно опасных последствий, состав преступления, предусмотренного ст. 242.1 УК РФ, отсутствует…»[1].

В противоположном случае Судебная коллегия Верховного Суда РФ отменила оправдательный приговор нижестоящего суда и отправила дело на новое рассмотрение, указав, что: *«…приведя в апелляционном приговоре заключение компьютерно-технической экспертизы относительно изъятого у Ш. системного блока "Zalman" и экспертизы содержащейся на нем информационной продукции, суд апелляционной инстанции сделал вывод о том, что скачивание порнографической информации с компьютера Ш. производилось другими пользователями в автоматическом режиме без его участия. Между тем указанный выше вывод не следует из заключений экспертов, согласно которым на системном блоке в ноябре 2009 года установлены программы "eMule" и "uTorrent". В директории "<...>" обнаружены видеоматериалы с порнографическими изображениями несовершеннолетних, в том числе лиц, не достигших 14-летнего возраста. Обмен файлами с другими пользователями из данной папки производился с помощью программ "uTorrent" и "eMule". Раздача информации с помощью программы "uTorrent" настраивается пользователем программы путем указания папок, из которых он разрешает скачивание информации. В программе "eMule" для организации обмена файлами пользователь указывает местонахождение включенных в раздачу файлов. Указанным способом из разрешенной Ш. к раздаче папки "<...>" передано другим пользователям 566 Гб информации…»*[2].

[1] Кассационное определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 06.07.2021 № 89-УД21-8-К7 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Кассационное определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 19.05.2022 № 47-УДп22-3-К6 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

Таким образом, учитывая положения п. 23 ППВС РФ от 15.12.2022 № 37, для правильной квалификации действий лица следует в каждом случае устанавливать, во-первых, наличие у него специальных знаний в области компьютерной техники и навыки работы в сети Интернет или соответствующее образование, во-вторых, осведомлено ли оно о функциях используемой программы-файлообменника, в-третьих, при необходимости назначать судебную экспертизу.

В свою очередь, согласно ППВС РФ от 15.12.2022 № 37 публичная демонстрация, осуществляемая как в прямом эфире, так и на личных страницах, страницах групп пользователей, тоже возможна несколькими способами: 1) открытый показ; 2) предоставление возможности просмотра материалов без возможности самостоятельного их использования.

Отметим, что закон предъявляет к демонстрации обязательный признак — публичность, следовательно, показ или предоставление возможности просмотра порнографического материала должны осуществляться среди широкой группы лиц (в групповых чатах различных мессенджеров с количеством участников в несколько десятков или даже сотен) либо неограниченного числа лиц[1].

Например, суд вынес в отношении Г. обвинительный приговор по п. «б» ч. 3 ст. 242 УК РФ за то, что он разместил на своей странице в социальной сети в открытом доступе файлы, содержащие порнографические материалы, предоставив неограниченному количеству пользователей возможность их просмотра и копирования[2].

Если подобные действия происходят в закрытых чатах или в конфиденциальной переписке с конкретным лицом, то ответ-

[1] Шаганова О. М. Особенности квалификации клеветы, совершенной публично с использованием информационно-телекоммуникационных сетей, включая сеть «Интернет» // Научный вестник Омской академии МВД России. 2023. № 2. С. 103–108.

[2] Приговор Орджоникидзевского районного суда г. Уфы Республики Башкортостан от 19 октября 2017 г. Д. № 1-314/2017. URL: https://sud-praktika.ru/precedent/467848.html (дата обращения: 08.05.2024).

ственность по ст. 242, 242.1 УК РФ за публичную демонстрацию не наступит.

В зависимости от того, что представляет предмет репоста в социальной сети и каким образом он осуществляется, может меняться деяние объективной стороны исследуемых преступлений, относящееся к обороту порнографических материалов. Так, если преступник, осуществляя репост материалов порнографического характера, отправляет их в личном сообщении, осуществляет их массовую рассылку либо выполняет репост ссылки для загрузки файлов, то это должно признаваться распространением таких материалов.

Если лицо совершает репост материалов, позволяющих на личной странице или на странице групп пользователей осуществлять их открытый показ либо предоставлять возможность их просмотра, то подобное выступает публичной демонстрацией.

К примеру, Судебная коллегия Верховного Суда РФ одним из доводов отмены решения нижестоящего суда кассационной инстанции и отправки дела на новое рассмотрение в отношении П. признала следующее: «…публичная демонстрация… заключается в открытом показе порнографических материалов, либо предоставление неограниченному числу лиц возможности просмотра таких материалов…, в том числе репост — размещение ссылки непосредственно на информацию в источнике первичного размещения…»[1].

Под приобретением материалов с порнографическими изображениями несовершеннолетних, совершенным с использованием информационно-телекоммуникационных сетей, в том числе сети Интернет, следует понимать любые способы их получения, связанные с использованием сети Интернет, например загрузка/скачивание на любой носитель (компьютерное устройство, карту памяти и т. д., в т. ч. с использованием специальной ком-

[1] Кассационное определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 08.12.2022 № 1-УДП22-10-К3 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

пьютерной программы) самостоятельно найденного материала либо пересланного кем-либо из пользователей и т. п. Не относятся к приобретению те случаи, когда лицо только ознакомилось (просмотрело) с видео-, фотофайлом, содержащими информацию порнографического характера, в сети Интернет и не сохранило копию на любой носитель (в т. ч. с использованием специальной компьютерной программы).

Единственное деяние, которое может быть совершено в сети Интернет как в отношении материалов, так и в отношении предметов порнографического характера, — это рекламирование, которое представляет собой распространение информации среди неопределенного круга лиц, совершаемое с целями: 1) привлечения внимания к объекту рекламирования; 2) формирования или поддержания интереса к нему; 3) продвижения его на рынке[1].

Поскольку составы преступлений, предусматривающих ответственность по ст. 242 и 242.1 УК РФ, являются альтернативными, следовательно, если в действиях виновного лица есть признаки нескольких деяний объективной стороны одновременно, то, во-первых, все они должны быть описаны в материалах дела и, во-вторых, квалификация должна осуществляться по одному факту п. «б» ч. 3 ст. 242 УК РФ или п. «г» ч. 2 ст. 242.1 УК РФ.

Например, Д. совершил приобретение, хранение в целях распространения, распространение материалов с порнографическими изображениями несовершеннолетних, совершенное в отношении лица, не достигшего четырнадцатилетнего возраста, с использованием средств массовой информации, в т. ч. информационно-телекоммуникационных сетей (включая сеть Интернет). Суд вынес

[1] 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» [Электронный ресурс]: постановление Пленума Верховного Суда Российской Федерации от 15.12.2022 № 37. Доступ из справ.-правовой системы «КонсультантПлюс».

в отношении него обвинительный приговор по п. «а», «г» ч. 2 ст. 242.1 УК РФ[1].

Совокупность возможна только в случае, если лицо совершило в любой последовательности преступления, предусмотренные п. «б» ч. 3 ст. 242 УК РФ и п. «г» ч. 2 ст. 242.1 УК РФ, независимо от того, был ли разрыв во времени между ними[2].

Таким образом, при квалификации незаконного оборота порнографических материалов или предметов, совершенного с использованием информационно-телекоммуникационных сетей, в т. ч. сети Интернет, необходимо, руководствуясь ППВС от 15.12.2022 № 37, устанавливать все обстоятельства содеянного, умысел виновного лица, наличие у него специальных знаний в области компьютерной техники и навыки работы в сети Интернет или соответствующее образование, его осведомленность о функциях используемой программы-файлообменника, а также при необходимости назначать судебную экспертизу.

[1] Приговор Коминтерновского районного суда г. Воронежа от 17 августа 2017 г. Д. № 1-533/2017. URL: https://sud-praktika.ru/precedent/468503.html (дата обращения: 08.05.2024).

[2] Подобное правило изложено: О судебной практике по делам о преступлениях против половой неприкосновенности и половой свободы личности [Электронный ресурс]: постановление Пленума Верховного Суда Российской Федерации от 14.12.2014 № 16, п. 9. Доступ из справ.-правовой системы «КонсультантПлюс».

ЗАКЛЮЧЕНИЕ

Проведенное исследование позволяет констатировать, что преступления в сфере информационно-телекоммуникационных технологий в настоящее время выступают наиболее распространенными и составляют большинство из всех регистрируемых деяний. В работе представлено уголовно-правовое предупреждение данных деяний, которое в первую очередь зависит от правильной квалификации и эффективности реализации предписаний уголовного закона. В связи с этим особое внимание авторами уделено разрешению проблем квалификации преступлений против личности, собственности, компьютерной информации, здоровья населения, общественной нравственности, совершаемых с использованием информационно-телекоммуникационных технологий.

Так, использование сети Интернет при совершении преступлений, связанных с преступной причастностью к самоубийству, характеризуется основными признаками объективной стороны доведения до самоубийства, склонения к совершению самоубийства или содействия его совершению, организации деятельности, направленной на побуждение к совершению самоубийства. В работе исследованы особенности, позволяющие произвести четкое разграничение между данными составами, а также представлены правила квалификации действий лица, одновременно содержащих признаки составов преступлений, предусмотренных п. «д» ч. 3 ст. 110^1 и ч. 2 ст. 110^2 УК РФ. Кроме того, в связи с существующими правоприменительными проблемами, связанными с отсутствием единообразной квалификации, сделан вывод о необходимости четких судебных разъяснений.

Также в работе исследованы проблемы квалификации клеветы, совершенной публично с использованием информационно-телекоммуникационных сетей, включая сеть Интернет, связанные с установлением предмета преступления, способа его совершения и моментом окончания преступления. Так, предмет преступления (клеветнические сведения) должен обладать сле-

дующими характеристиками: быть ложным и порочить честь и достоинство лица либо подрывать репутацию.

Объективная сторона ч. 2 ст. 128^1 УК РФ проявляется в виде публичного способа распространения клеветы, например размещение ее на сайтах, форумах или в блогах, массовая рассылка электронных сообщений и иные подобные действия, в т. ч. рассчитанные на последующее ознакомление с информацией других лиц. Вместе с тем в рамках уголовного дела необходимо доказать, что размещение клеветнических сведений публично было осуществлено конкретным лицом (к примеру, владельцем аккаунта или другим пользователем аккаунта, действовавших не от своего имени (от имени другого человека или анонимно) и т. п.).

Момент окончания преступления зависит от вида распространяемых сведений. Если это электронная информация, то преступление окончено в момент ее публикации (размещения), т. е. когда появляется возможность у третьего человека с ней ознакомиться. Клевета, передающаяся при помощи инструментов IP-телефонии, окончена с момента осуществления видео-, аудиозвонка, когда у третьего лица возникает возможность ее воспринять.

Правильная квалификация преступлений против собственности, совершаемых с использованием цифровых средств, зависит от того, каким способом производится изъятие. В частности, если роль потерпевшего в передаче имущества активная и, будучи введенным в заблуждение, он переводит самостоятельно денежные средства, то квалификация должна проводиться по составам мошенничества. При пассивной роли потерпевшего вменению подлежит ст. 158 УК РФ.

При квалификации неправомерного доступа к компьютерной информации правоприменительным органам необходимо особое внимание уделить установлению: предмета преступления — охраняемой законом компьютерной информации — путем указания на тот нормативный правовой акт, в соответствии с которым доступ был ограничен, либо описания мер, предпринятых обладателем информации для ее сохранности; деяния в виде неправомерного доступа, означающего не только получение и использование компьютерной информации, но и возможность совершения таких действий; преступных последствий в виде копи-

рования, модификации, блокирования, уничтожения информации.

Для верной квалификации преступления, предусмотренного ст. 273 УК РФ, необходимо установить:

1) предмет преступления в виде компьютерной программы или иной компьютерной информации должен обладать признаками вредоносности, т. е. способностью уничтожать, блокировать, модифицировать, копировать компьютерную информацию или нейтрализовать средства защиты такой информации;

2) способ совершения деяния — создание, распространение, использование предмета преступления. При этом независимо от того, совершается ли несколько из перечисленных действий одновременно либо имеет место только одно из них, квалификация осуществляется только по ст. 273 УК РФ. В том случае, если лицо использует вредоносную компьютерную программу для совершения иного преступления (например, ст. 137, 138, 159^6 УК РФ и т. п.), требуется квалификация преступлений по совокупности со ст. 273 УК РФ;

3) признак заведомости по отношению к характеристике предмета преступления, который доказывается путем указания в материалах дела на уровень образования преступника либо наличие специальных знаний и/или навыков, позволяющих ему осознавать вредоносное предназначение программы или иной информации.

При квалификации деяния по ст. 274 УК РФ правоприменительным органам необходимо особое внимание уделять установлению следующих обстоятельств: наличие специального порядка обращения с компьютерной информацией, закрепленного в нормативных правовых актах РФ, субъектов РФ либо локальных актах организации; наличие у виновного лица обязанностей соблюдения специальных правил и его ознакомление с ними; наступление преступных последствий, с которыми законодатель связывает момент окончания преступления и возможность привлечения к уголовной ответственности.

Проблемы квалификации незаконного оборота наркотических средств, совершаемых с использованием IT-технологий, в своей основе связаны с расширением Верховным Судом РФ понятия сбыта как деятельности по реализации данных предме-

тов, что повлияло как на определение видов соучастников преступления, стадий совершения преступления, а также момента окончания.

При квалификации незаконного оборота порнографических материалов или предметов, совершенного с использованием информационно-телекоммуникационных сетей, в т. ч. сети Интернет, необходимо устанавливать все обстоятельства содеянного, умысел виновного лица, наличие у него специальных знаний в области компьютерной техники. Объективная сторона составов преступлений, предусмотренных ст. 242, 242^1 УК РФ, представлена альтернативными действиями (приобретение, публичная демонстрация, рекламирование). При этом, несмотря на то, что совершение любого из названных действий уже образует оконченное преступление, правоприменительным органам следует расписывать признаки каждого деяния отдельно.

СОДЕРЖАНИЕ

Учебное издание

Ботвин Илья Викторович, **Ермакова** Ольга Владимировна,
Шаганова Ольга Михайловна, **Малетина** Мария Александровна

ОСОБЕННОСТИ КВАЛИФИКАЦИИ И ПРЕДУПРЕЖДЕНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Учебное пособие

Редактура	О. Н. Татарниковой, Е. Г. Авдюшкина
Компьютерная верстка, дизайн обложки	О. Н. Татарниковой

Лицензия ЛР № 02213552 от 14.07.1999 г.
Лицензия Плр № 020109 от 15.07.1999 г.

Подписано в печать 06.09.2024 г. Формат 60х90 1/16.
Ризография. Усл.п.л. 6,3 п.л. Тираж 37 экз. Заказ № 357.
Барнаульский юридический институт МВД России.
Научно-исследовательский и редакционно-издательский отдел.
656038, Барнаул, ул. Чкалова, 49; бюи.мвд.рф.