ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САМАРСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
УНИВЕРСИТЕТ ИМЕНИ АКАДЕМИКА С. П. КОРОЛЕВА»
(САМАРСКИЙ УНИВЕРСИТЕТ)

На правах рукописи

Корпеев Ата Гельдыевич

ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ ПО УГОЛОВНОМУ ЗАКОНОДАТЕЛЬСТВУ РОССИЙСКОЙ ФЕДЕРАЦИИ И ТУРКМЕНИСТАНА: СРАВНИТЕЛЬНО-ПРАВОВОЕ ИССЛЕДОВАНИЕ

5.1.4. Уголовно-правовые науки

Диссертация на соискание ученой степени кандидата
юридических наук

Научный руководитель: доктор юридических наук, профессор,

заслуженный юрист Российской Федерации

Безверхов Артур Геннадьевич

Самара – 2025

ОГЛАВЛЕНИЕ

Введение 3

Глава 1. Социально-правовой анализ преступлений в сфере компьютерной информации и иных преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (технологий) 30

1.1. Общая характеристика преступлений в сфере компьютерной информации и иных преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (технологий), по уголовному законодательству Российской Федерации 30

1.2. Общая характеристика преступлений в сфере компьютерной информации и иных преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (технологий), по уголовному законодательству Туркменистана 50

1.3. Состояние и динамика преступлений в сфере компьютерной информации и иных преступлений, совершаемых с использованием информационно – телекоммуникационных сетей (технологий), в Российской Федерации и Туркменистане 63

Глава 2. Соотношение основных составов преступлений в сфере компьютерной информации по современному уголовному законодательству России и Туркменистана 81

2.1. Особенности объективных признаков преступлений в сфере компьютерной информации по современному уголовному законодательству России и Туркменистана 81

2.2. Специфика субъективных признаков преступлений в сфере компьютерной информации по современному уголовному законодательству России и Туркменистана 113

Глава 3. Соотношение квалифицирующих и особо квалифицирующих признаков преступлений в сфере компьютерной информации по современному уголовному законодательству России и Туркменистана 129

3.1. Соотношение квалифицирующих признаков преступлений в сфере компьютерной информации по современному уголовному законодательству России и Туркменистана 129

3.2. Соотношение особо квалифицирующих признаков преступлений в сфере компьютерной информации по современному уголовному законодательству России и Туркменистана 132

Заключение 154

Список литературы 163

Приложение 1 188

Приложение 2 192

ВВЕДЕНИЕ

Актуальность темы диссертационного исследования. Развитие нового социума непосредственно связано с возрастающей ролью информационной среды, которая органически включает в себя такие составные компоненты, как компьютерная информация, электронные (цифровые) устройства и информационно-телекоммуникационные сети. Появление информационных методов оптимизации социальной жизнедеятельности открывает путь к еще большему – планированию и развитию элементов информационно-технологического процесса – инноваций технических средств, основной функцией которых является обеспечение инновационного прогресса и защиты информационно-телекоммуникационного (кибернетического) пространства[1].

«На фоне кибервызовов XXI века повышенный интерес вызывает соотношение механизмов уголовно-правового регулирования в сфере компьютерной информации, функционирующих в России и независимом со статусом постоянного нейтралитета Туркменистане, – «в двух современных державах, на протяжении более ста лет (1881-1991 гг.) объединенных в границах единой государственности: сначала Российской империи, а после – Союза Советских Социалистических Республик»[2].

Выбор стран для осуществления сравнительно-правового исследования обусловлен также причинами международно-правового характера. Несмотря на свой нейтральный статус, Туркменистан является ассоциированным членом Содружества Независимых Государств и активно интегрируется с Российской Федерацией в вопросах противодействия преступлениям в сфере

---

[1] См.: Григорян Г.Р. Мошенничество в сфере компьютерной информации: проблемы криминализации, законодательной регламентации и квалификации: диссертация ... кандидата Юридических наук: 12.00.08. Самара, 2021. С.3.

[2] См.: Аминов, И. И., Становление и развитие правовой системы Туркменистана: монография / И. И. Аминов. — Москва: Русайнс, 2024. — 378 с. [Электронный ресурс]. URL: https://book.ru/book/953582 (дата обращения: 13.05.2025).

компьютерной информации и иным преступлениям, совершаемым с использованием информационно-телекоммуникационных сетей (технологий). За четверть века независимости и нейтралитета Туркменистана между Российской Федерацией и Туркменистана – одним из ключевых государств Центральной Азии - подписан ряд правовых документов в сфере предупреждения указанных правонарушений. Это Соглашение о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий от 28 сентября 2018 г.[1], Соглашение между Правительством Российской Федерации и Правительством Туркменистана о сотрудничестве в области обеспечения международной информационной безопасности от 5 апреля 2019 г.[2]

Помимо международно-правовых документов и межгосударственных соглашений криминального цикла в обеих странах действует целый кластер политико-правовых источников в сфере информационной безопасности. Это – Доктрина информационной безопасности в Российской Федерации, утвержденная Указом Президента Российской Федерации от 5 декабря 2016 г. № 646[3], Стратегия развития информационного общества в Российской Федерации на 2017 – 2030 годы, утвержденная Указом Президента Российской Федерации от 9 мая 2017 г. № 203[4], Меры по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена, утвержденные Указом Президента Российской Федерации от 17 марта 2008 г.

---

[1] Соглашение о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий от 28 сентября 2018 года. [Электронный ресурс]. URL: http://publication.pravo.gov.ru/Document/View/0001202207180005.

[2] Бюллетень международных договоров октябрь 2019, № 10, стр. 63-68, Официальный интернет-портал правовой информации. [Электронный ресурс]. URL: www.pravo.gov.ru. 13.06.2019.

[3] Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента РФ от 5.12.2016 № 646. [Электронный ресурс]. URL: https://base.garant.ru/71556224/.

[4] Стратегия развития информационного общества в Российской Федерации на 2017 – 2030 годы, утвержденной Указом Президента РФ от 9.05.2017 № 203. [Электронный ресурс]. URL: tps://base.garant.ru/71670570/.

№ 351[1], Стратегия национальной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 2 июля 2021 г. № 400[2], Постановление Президента Туркменистана об обеспечении кибербезопасности от 19 января 2024 г.[3], Государственная программа по обеспечению кибербезопасности Туркменистана на 2022-2025 гг., утвержденная Указом Президента Туркменистана от 2 марта 2022 г. № 2623[4] и др.

Как отметил Президент Российской Федерации В.В. Путин, выступая на конференции «Путешествие в мир искусственного интеллекта», «с внедрением искусственного интеллекта в науку, в образование, здравоохранение – да во все сферы нашей жизни, человечество начинает новую главу своего существования»[5]. При этом, «естественно, должны быть сведены к минимуму любые угрозы для граждан для сохранения персональных данных»[6]. Президент Туркменистана С.Г. Бердымухамедов на саммите лидеров стран СНГ подчеркнул, что «странам следует активно интегрироваться в сфере выработки механизмов по противодействию преступлениям в сфере компьютерной информации»[7].

---

[1] Меры по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена, утвержденные Указом Президента РФ от 17.03.2008 № 351. [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_75586/

[2] Стратегия национальной безопасности Российской Федерации, утвержденная Указом Президента РФ от 02.07.2021 № 400. [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_389271/.

[3] Постановление об обеспечении кибербезопасности, утвержденное Президентом Туркменистана от 19.01.2024. [Электронный ресурс]. URL: https://asmannews.ru/news/2194/prezident-turkmenistana-podpisal-postanovlenie-ob-obespecenii-kiberbezopasnosti.

[4] Государственная программа по обеспечению кибербезопасности Туркменистана на 2022-2025 годы, утвержденная Президентом Туркменистана от 02.03.2022 № 2623. [Электронный ресурс]. URL: https://turkmen.news/wp-content/uploads/2022/09

[5] Из выступления Президента Российской Федерации В.В. Путина на конференции «Путешествие в мир искусственного интеллекта» 24.11.2023. [Электронный ресурс]. URL: https://www.1tv.ru/news/2023-11-24/465777vladimir_putin_vystupil_na_plenarnom_zasedanii_konferentsii_posvyaschennoy_iskusstvennomu_intellektu

[6] Из выступления Президента Российской Федерации В.В. Путина на конференции «Путешествие в мир искусственного интеллекта» 24.11.2023. [Электронный ресурс]. URL: https://www.1tv.ru/news/2023-11-24/465777vladimir_putin_vystupil_na_plenarnom_zasedanii_konferentsii_posvyaschennoy_iskusstvennomu_intellektu.

[7] Президент Туркменистана рассказал главам СНГ о киберугрозах и газопроводах. [Электронный ресурс]. URL: https://turkmen.news/prezident-turkmenistana-rasskazal-glavam-sng-o-kiberugrozah-i-gazoprovodah/.

По данным Главного информационно-аналитического центра Министерства внутренних дел Российской Федерации в 2020 г. зарегистрировано 510 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий, что на 73,4% больше, чем за аналогичный период прошлого года; при этом 300 тыс. (58,8%) таких преступлений совершены с использованием сети «Интернет», 4498 тыс. (6 %) - в сфере компьютерной информации[1]. В 2021 г. совершено 517,7 тысяч данных преступлений, что на 1,4 % больше, чем за аналогичный период прошлого года; при этом 351,5 тыс. (67,9%) совершены с использованием сети «Интернет», 6869 тыс. (3 %) – в сфере компьютерной информации[2]. В 2022 г. - 522,1 тыс., что на 0,8 % больше, чем за аналогичный период прошлого года, при этом 381,1 тыс. (73%) совершенны с использованием сети «Интернет», 10027 тыс. (4%) – в сфере компьютерной информации[3]. В 2023 г. - 677 тыс., что на 29,5% больше, чем за аналогичный период прошлого года, при этом 526 тыс. (77,8%) совершены с использованием сети «Интернет», 37 тыс. (8%) – в сфере компьютерной информации[4]. В 2024 г. - 765,4 тыс., что на 13.1 % больше, чем за аналогичный период прошлого года, при этом 649,1 тыс. (84,8%) совершены с использованием сети «Интернет», 52 тыс. (8%) - в сфере компьютерной информации[5].

По открытым статистическим данным и анализу динамики цифровых преступлений различной формации в Туркменистане ежемесячно от общего числа преступлений фиксируется 48 % компьютерных атак с помощью

---

[1] Состояние преступности в Российской Федерации за январь - декабрь 2020 года. [Электронный ресурс]. URL: https://xn--b1aew.xn--p1ai/reports/item/22678184/ (дата обращения: 26.03.2025).
[2] Состояние преступности в Российской Федерации за январь - декабрь 2021 года. [Электронный ресурс]. URL: https://xn--b1aew.xn--p1ai/reports/item/28021552/ (дата обращения: 26.03.2025).
[3] Состояние преступности в Российской Федерации за январь - декабрь 2022 года. [Электронный ресурс]. URL: https://xn--b1aew.xn--p1ai/reports/item/35396677/ (дата обращения: 26.03.2025)
[4] Состояние преступности в Российской Федерации за январь - декабрь 2023 года. [Электронный ресурс]. URL: https://xn--b1aew.xn--p1ai/reports/item/47055751/ (дата обращения: 26.03.2025).
[5] Состояние преступности в Российской Федерации за январь - декабрь 2024 года. [Электронный ресурс]. URL: https://xn--b1aew.xn--p1ai/reports/item/60248328/ (дата обращения: 26.03.2025).

программ-вымогателей, 25% веб-угроз, 27 % локальных атак (банки и государственные организации)[1].

«С теоретико-прикладной точки зрения изучение «уголовно-правовых преобразований в бывших республиках Советского Союза, а ныне суверенных государствах, имеет для отечественной юридической науки и практики особую ценность, в том числе и в части влияния исторического прошлого двух стран на современную связь их уголовно-правовых систем»[2] в сфере компьютерной информации и взаимозаимствование положительного законодательного и правоприменительного опыта в области предупреждения анализируемых деликтов»[3]. Сравнительно-правовой анализ составов преступлений в сфере компьютерной информации и иных преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (технологий), по уголовному законодательству России и Туркменистана, указывает на тот факт, что до 2022 г. система построения составов преступлений в сфере компьютерной информации в Уголовном кодексе Российской Федерации[4] и Уголовном кодексе Туркменистана[5] была идентичной. Идентичным в сравниваемых кодификациях было и число состав преступлений в сфере компьютерной информации. Однако в 2022 г. УК Туркменистана претерпел отдельные системно-структурные и содержательные модификации в части ответственности за преступления в сфере компьютерной информации, что требует комплексного юридико-технического и сравнительно-правового анализа.

---

[1] Статистика киберугроз в Туркменистане. [Электронный ресурс]. URL: https://statistics.securelist.com/ru/country/turkmenistan/ransomware/day (дата обращения: 26.03.2025).
[2] Аминов, И. И., Становление и развитие правовой системы Туркменистана: монография / И. И. Аминов. — Москва: Русайнс, 2024. — 378 с. [Электронный ресурс]. URL: https://book.ru/book/953582 (дата обращения: 13.05.2025).
[3] Аминов, И. И., Становление и развитие правовой системы Туркменистана: монография / И. И. Аминов. — Москва: Русайнс, 2024. — 378 с. [Электронный ресурс]. URL: https://book.ru/book/953582 (дата обращения: 13.05.2025).
[4] Далее – УК РФ.
[5] Далее – УК Туркменистана.

Кроме того, обращают на себя внимание проблемы понятийно-категориального аппарата, используемого при описании преступлений в сфере компьютерной информации и иных преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (технологий), а также применение законодателем отдельных правил юридической техники. Так, в УК Туркменистана отсутствуют легальные дефиниции понятий «охраняемая законом информация», «компьютерная информация». Обусловленные информационно-технологическими образованиями сложности уголовно-правовых формулировок, бланкетный характер соответствующих нормативных правовых положений, построение системы преступлений в сфере компьютерной информации и иных преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (технологий), приводят к ошибкам в квалификации анализируемых и смежных с ними уголовно наказуемых деяний. Также в Туркменистане отсутствуют общие судебные разъяснения Верховного Суда Туркменистана о судебной практике по делам о рассматриваемых преступлениях.

В современной российской и туркменской уголовно-правовой науке окончательно не решен вопрос о социально-правовой природе преступлений в сфере компьютерной информации и иных преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (технологий). Прежде всего, это видно из множественности определений понятий таких посягательств: «киберпреступления», «преступления в сфере информационных технологий», «цифровые преступления», «преступления, совершенные с использованием информационно-телекоммуникационных сетей», «информационные преступления», «преступления в сфере информационной безопасности», «компьютерные преступления» и др.

Актуальность темы диссертации обуславливается также недостаточной изученностью в отечественной уголовно-правовой доктрине механизма уголовно-правовой охраны отношений в сфере компьютерной информации в

Туркменистане. Более того, в настоящее время отсутствуют монографические исследования, посвященные сравнительно-правовому анализу составов преступлений в сфере компьютерной информации по уголовному праву России и Туркменистана.

Наконец, особое внимание к проблематике диссертационного исследования определяет следующее обстоятельство. Распространение преступлений в сфере компьютерной информации и иных преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (технологий), не ограничивается пределами одного государства. Эти криминальные деликты представляют собой масштабную транснациональную угрозу, которая требует совместных усилий многих стран и международного сообщества в целом. Активное участие в этом противостоянии принимают Российская Федерация и Туркменистан, государства с общей исторической памятью и судьбой. Для диссертанта, уроженца и гражданина Туркменистана, в 2015 г. окончившего совместную туркмено-российскую среднюю общеобразовательную школу имени А.С. Пушкина в г. Ашхабад, а в последующем успешно освоившего в Самарском университете программы трех уровней высшего юридического образования (бакалавриат-магистратура-аспирантура) и получившего гражданство Российской Федерации, настоящее теоретико-прикладное исследование – посильный вклад в дальнейшее совместное развитие информационной безопасности своей большой и малой Родины.

Вышеуказанные причины и обстоятельства обуславливают актуальность диссертационного исследования, обосновывают необходимость проведения сравнительного правового анализа уголовного законодательства Российской Федерации и Туркменистана об ответственности за преступления в сфере компьютерной информации и практики его применения.

Степень научной разработанности темы исследования. Теоретическую базу сравнительно правового исследования составляют труды

российских, зарубежных ученых-юристов, посвященные исследованию проблем квалификации, социально-правовой природы преступлений в сфере компьютерной информации и иных преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (технологий), механизму уголовно-правового обеспечения информационной безопасности, теоретико-прикладным проблемам в сфере уголовно-правового противодействия вышеуказанным преступлениям.

Между тем, основные вопросы и релевантные учения законодательной регламентации и квалификации преступлений в сфере компьютерной информации и иных преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (технологий), отражены в научных трудах российских ученых: И.И. Аминова, Н.А. Агешкиной, И.А. Александровой, И.Р. Бегишева, Л.А. Букалеровой, А.Г. Безверхова, М.А. Беляева, Ю.В. Беляниновой, И.И. Бикеева, Л.М. Болсуновской, С.В. Бородина, С.Д. Бражникова, В.Б. Вехова, А.Б. Волеводз, Ю.В. Грачевой М.С. Гаджиева, А.В. Гладких, Р.Р. Гайфутдинова, Г.Р. Григоряна, К.Н. Евдокимова, М.Ю. Дворецкого, В.М. Елина, О.В. Ермаковой, М.А. Ефремовой, Л.В. Иногамовой-Хегай, Н.Ш. Козаева, А.А. Комарова, С.М. Кочои, Н.А. Лихачева, Н.А. Лопашенко, Е.А. Маслаковой, В.А. Мазурова, С.С. Медведева, И.А. Мусьял, М. Гусейн Наджафи, Д.А. Овсюкова, В.Ю. Окружко, М.А. Простосердова, Д.В. Пучкова, Е.А. Русскевича, Д.В. Савельева, О.М. Сафонова, Т.М. Судаковой, Н.А. Селиванова, А.В. Серебренниковой, Н.Ю. Скрипченко, Э.Л. Сидоренко, Е.А. Соловьевой, М.Д. Фролова, З.И. Хисамова, А.А. Ходусова, В.В. Челнокова, А.Ю. Чупровой, А.И. Чучаева, С.С. Шахрая, Г.Ф. Шипулина, А.А. Южина, И.А. Юрченко, П.С. Яни и др., а также туркменских ученых: Т.А. Джумаева, Д.Д. Ораздурдыевой, М.Х. Мередова.

Для исследования социально-экономических аспектов указанных преступлений изучены научные работы К.С. Кингстона, З. Иня, Г. Сюэ, П. Го, Ф. Варезе и других исследователей.

Актуальные теоретико-прикладные проблемы в сфере уголовно-правового противодействия преступлениям в сфере компьютерной информации и иным преступлениям, совершаемым с использованием информационно-телекоммуникационных сетей (технологий), комплексно проанализированы в монографических работах И.Р. Бегишева и И.И. Бикеева «Преступления в сфере обращения цифровой информации» (2020 г.), В.М. Быкова и В.Н. Черкасова «Преступления в сфере компьютерной информации» (2015 г.), Е.А. Русскевича «Уголовное право и «цифровая преступность»: проблемы и решения» (2019 г.).

Механизму уголовно-правового обеспечения информационной безопасности посвящены докторские диссертации К.Н. Евдокимова «Противодействие компьютерной преступности: теория, законодательство, практика» (2022 г.), М.А. Ефремовой «Уголовно-правовая охрана информационной безопасности» (2018 г.), Д.В. Пучкова «Уголовно-правовая модель защиты телекоммуникаций от преступных посягательств: проблемы теории и практики» (2022 г.), Е.А. Русскевича «Дифференциация ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий, и проблемы их квалификации» (2021 г.).

Объектом диссертационного исследования являются общественные отношения, возникающие в связи с совершением преступлений в сфере компьютерной информации и иных преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (технологий), в Российской Федерации и Туркменистане.

Предмет диссертационного исследования состоит из совокупности внутригосударственных и международных нормативных правовых актов,

теоретико-прикладных проблем уголовно-правовой науки о преступлениях в сфере компьютерной информации и иных преступлениях, совершаемых с использованием информационно-телекоммуникационных сетей (технологий), в Российской Федерации и Туркменистане, включающих:

– научные теории, основанные на сравнительном анализе уголовно-правовых норм УК РФ и УК Туркменистана о преступлениях в сфере компьютерной информации;

– нормы российского и туркменского уголовного законодательства об ответственности за преступления в сфере компьютерной информации и иные преступления, совершаемые с использованием информационно-телекоммуникационных сетей (технологий), и практики их применения;

– международные нормативные правовые акты о преступлениях в сфере компьютерной информации и иных преступлениях, совершаемых с использованием информационно-телекоммуникационных сетей (технологий);

– особенности социально-правовой природы, законодательной регламентации (в том числе юридико-технического строения разделов, глав и статей уголовного законодательства Российской Федерации и Туркменистана) и квалификации преступлений в сфере компьютерной информации и иных преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (технологий);

– особенности и механизмы внутриотраслевого и межотраслевого взаимодействия положений УК РФ и УК Туркменистана об ответственности за преступления в сфере компьютерной информации и иные преступления, совершаемые с использованием информационно-телекоммуникационных сетей (технологий);

– специфика соотношения основных, квалифицированных и особо квалифицированных составов преступлений в сфере компьютерной информации по современному уголовному законодательству России и Туркменистана;

– фактологический материал, закономерности и тенденции состояния и динамики преступлений в сфере компьютерной информации и иных преступлений, совершаемых с использованием информационно – телекоммуникационных сетей (технологий), в Российской Федерации и Туркменистане.

Цель диссертационного исследования. На основании проведенного сравнительно-правового исследования, установив унифицированные и специфические аспекты уголовно-правового противодействия преступлениям в сфере компьютерной информации и иным преступлениям, совершаемым с использованием информационно–телекоммуникационных сетей (технологий), в Российской Федерации и Туркменистане, сформировать научно обоснованные положения о концептуальных подходах к уголовно-правовому противодействию преступлениям в сфере компьютерной информации и иным преступлениям, совершаемым с использованием информационно-телекоммуникационных сетей (технологий), в Российской Федерации и Туркменистане, выработать предложения по дальнейшему развитию общего учения о преступлениях в сфере компьютерной информации, обосновать целесообразность заимствования положительного опыта уголовно-правового предупреждения анализируемых деликтов в обеих странах для усовершенствования концепций построения и применения уголовного законодательства России и Туркменистана об ответственности за преступления в сфере компьютерной информации.

Для достижения данной цели поставлены следующие **задачи**:

– определить социально-правовую природу преступлений в сфере компьютерной информации и иных преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (технологий);

– осуществить компаративный анализ состояния и динамики преступлений в сфере компьютерной информации и иных преступлений,

совершаемые с использованием информационно-телекоммуникационных сетей (технологий);

– провести социально-правовой анализ признаков составов преступлений в сфере компьютерной информации и иных преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (технологий), по уголовному законодательству Российской Федерации и Туркменистана;

– выявить особенности соотношения объективных и субъективных признаков составов преступлений в сфере компьютерной информации по уголовному законодательству Российской Федерации и Туркменистана;

– провести сравнение квалифицирующих и особо квалифицирующих признаков преступлений в сфере компьютерной информации по уголовному законодательству Российской Федерации и Туркменистана;

– разработать рекомендации по совершенствованию уголовно-правовой теории и практики в части ответственности за преступления в сфере компьютерной информации и иные преступления, совершаемые с использованием информационно-телекоммуникационных сетей (технологий) по уголовному законодательству Российской Федерации и Туркменистана.

Методологическая основа диссертации. В целях рассмотрения особенностей предмета исследования, а также достижения целей и решения задач диссертационного исследования сформирована методологическая база из общенаучных и специальных методов исследования, способствующих многостороннему и достоверному исследованию.

С помощью методов анализа и синтеза были исследованы основные многосторонние компоненты объекта исследования. Посредством применения вышеуказанных методов рассмотрена социально-правовая сущность преступлений в сфере компьютерной информации и иных преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (технологий), в Российской Федерации и Туркменистане; разработаны отдельные категории в системе понятийно-категориального аппарата,

используемого в целях противодействия преступлениям в сфере компьютерной информации.

Посредством применения историко-правового подхода рассмотрен генезис положений уголовного законодательства Российской Федерации и Туркменистана о преступлениях в сфере компьютерной информации и иных преступлениях, совершаемых с использованием информационно-телекоммуникационных сетей (технологий).

Формально-юридический метод использован для исследования международного права в сфере высоких технологий и информационной безопасности, уголовно-правового материала Российской Федерации и Туркменистана о преступлениях в сфере компьютерной информации и иных преступлениях, совершаемых с использованием информационно-телекоммуникационных сетей (технологий), в части установления значения основных дефиниций, правовых категорий, принципов законодательной техники.

Статистический метод применялся при исследовании динамики преступлений в сфере компьютерной информации и иных преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (технологий), в Российской Федерации и Туркменистане; судебной практики по делам о вышеуказанных преступлениях.

На основе применения методов дедукции и индукции сформулированы основные выводы сравнительно-правового исследования, а также сформированы общие и отличительные особенности уголовно-правового регулирования преступлений в сфере компьютерной информации и иных преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (технологий), в Российской Федерации и Туркменистане.

Социологический метод применен при проведении социологического опроса среди сотрудников правоохранительных органов, судебной системы,

ученых-юристов, научных сотрудников по актуальным вопросам диссертационного исследования.

Применение метода правового моделирования позволило рассмотреть возможность перенесения опыта правовой системы Российской Федерации в вопросе уголовно-правового регулирования преступлений в сфере компьютерной информации и иных преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (технологий), в правовую систему Туркменистана и наоборот.

В основу настоящего исследования положен сравнительно-правовой подход. Метод сравнительного правоведения применен в качестве основного методологического инструментария для установления особенностей развития современного уголовного законодательства Российской Федерации и Туркменистана о преступлениях в сфере компьютерной информации и иных преступлениях, совершаемых с использованием информационно-телекоммуникационных сетей (технологий).

Теоретическую основу диссертационного исследования составляют труды российских, туркменских и зарубежных ученых-юристов по уголовному праву, криминологии, криминалистике, международному праву, теории права, а также научные изыскания по истории царского и советского периодов, истории развития советского уголовного законодательства и современного уголовного законодательства Российской Федерации и Туркменистана.

Теоретическая и практическая значимость диссертации связана с решением проблем научного, законотворческого и правоприменительного характера. Отдельные вопросы квалификации, законодательной техники и уголовной ответственности за преступления в сфере компьютерной информации и иные преступления, совершаемые с использованием информационно-телекоммуникационных сетей (технологий), комплексно анализируются в уголовно-правовой науке Российской Федерации и

Туркменистана. Вместе с тем, проблемы сопоставления накопленного опыта законотворческой и правоприменительной деятельности России и Туркменистана в области уголовно-правового противодействия преступлениям в сфере компьютерной информации и иным преступлениям, совершаемым с использованием информационно-телекоммуникационных сетей (технологий), относятся к числу малоисследованных.

Выработанные в ходе диссертационного исследования результаты способствуют развитию современной теории о преступлениях в сфере компьютерной информации и иных преступлениях, совершаемых с использованием информационно-телекоммуникационных сетей (технологий). В диссертационном исследовании определена социально-правовая сущность преступлений в сфере компьютерной информации и иных преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (технологий). Вместе с тем в диссертационном исследовании разработан релевантный понятийно-категориальный аппарат преступлений, предусмотренных главой 28 УК РФ и главой 33 УК Туркменистана.

Результаты исследования могут найти применение в преподавании курсов «Уголовное право», «Криминология», «Преступления против общественной безопасности», «Преступления в сфере компьютерной информации», «Информационное право».

Практическая значимость диссертационного исследования обусловлена возможностью дальнейшего применения основных теоретико-прикладных результатов диссертационного исследования в развитии учения уголовно-правовой науки Российской Федерации и Туркменистана о преступлениях в сфере компьютерной информации и иных преступлениях, совершаемых с использованием информационно-телекоммуникационных сетей (технологий), а также в совершенствовании законодательной и правоприменительной деятельности в обеих странах. Основные результаты работы направлены в Верховный Суд Туркменистана и юридический институт Туркменского

государственного университета имени Махтумкули для использования в правоприменительной, научной и образовательной сферах.

Эмпирическая основа диссертационного исследования представлена статистическими данными, подготовленными ГИАЦ МВД РФ и Государственным комитетом Туркменистана по статистике, статистическими данными «Лаборатории «Касперского» за период 2020–2024 гг, нормативными правовыми актами Российской Федерации и Туркменистана, определениями Конституционного Суда РФ, постановлениями Пленума Верховного Суда РФ, изученными 70 приговорами, вынесенными по уголовным делам о преступлениях в сфере компьютерной информации и иных преступлениях, совершаемых с использованием информационно-телекоммуникационных сетей (технологий), результатами социологического опроса 110 практических работников (адвокатов, сотрудников правоохранительных органов, судебной системы, преподавателей и научных работников университетов) по актуальным вопросам диссертационного исследования.

Научная новизна диссертации предопределена выбором темы настоящей работы и состоит в том, что это первое в истории уголовно-правовой науки России и Туркменистана сравнительно-правовое исследование положений российского и туркменского уголовного законодательства о преступлениях в сфере компьютерной информации и иных преступлениях, совершаемых с использованием информационно-телекоммуникационных сетей (технологий). В процессе сравнительно-правового исследования разработаны научные основы построения составов преступлений в сфере компьютерной информации с учетом специфики уголовного права России и Туркменистана, а также теоретические модели применения положений УК РФ и УК Туркменистана об уголовной ответственности за преступления в сфере компьютерной информации и иные

преступления, совершаемые с использованием информационно-телекоммуникационных сетей (технологий).

В диссертации решается комплекс теоретико-прикладных вопросов уголовно-правового противодействия преступлениям в сфере компьютерной информации и иным преступлениям, совершаемым с использованием информационно-телекоммуникационных сетей (технологий). Посредством сравнительно-правового подхода сопоставляется действующее уголовное законодательство Российской Федерации и Туркменистана в части ответственности за указанные уголовно наказуемые нарушения, раскрывается их социально-правовая природа, устанавливается общее и особенное в объективных, субъективных, квалифицирующих и особо квалифицирующих признаках анализируемых преступных посягательств.

На основании проведенного исследования выработаны авторские предложения в части уточнения используемого в уголовном праве соответствующего понятийно-категориального аппарата, совершенствования правоприменительной практики и оптимизации уголовного законодательства Российской Федерации и Туркменистана об ответственности за преступления в сфере компьютерной информации и иные преступления, совершаемые с использованием информационно-телекоммуникационных сетей (технологий).

Развитие релевантного научного знания о правилах построения и применения положений УК РФ и УК Туркменистана о преступлениях в сфере компьютерной информации и иных преступлениях, совершаемых с использованием информационно-телекоммуникационных сетей (технологий) достигается:

– разработкой релевантной системы научного понимания категорий уголовно-правового характера «преступления в сфере компьютерной информации», «преступления, совершаемые с использованием информационно-телекоммуникационных сетей (технологий); «компьютерные преступления» и соотношении сформулированных дефиниций в понятийно-

категориальном ряду уголовного права в области информационной безопасности;

– исследованием соотношения объективных, субъективных, квалифицирующих и особо квалифицирующих признаков составов преступлений в сфере компьютерной информации по УК РФ и УК Туркменистана;

– авторскими рекомендациями по построению разделов, глав и статей российского и туркменского уголовных законов об ответственности за преступления в сфере компьютерной информации и практики их применения.

Основные положения, выносимые на защиту.

1. На основе разработанного понятийно-категориального ряда «преступления в сфере компьютерной информации» - «преступления, совершаемые с использованием информационно-телекоммуникационных сетей (технологий)» - «компьютерные преступления» показано, что преступления в сфере компьютерной информации и иные преступления, совершаемые с использованием информационно-телекоммуникационных сетей (технологий), обладают сложной социально-правовой природой, обусловленной прежде всего спецификой определения объективных признаков таких деяний, в том числе средств и способов совершения преступления, места совершения преступления. К числу усложняющих компонентов социально-правовой природы таких преступлений следует относить также многообъектность. По уголовному законодательству Российской Федерации и Туркменистан родовым объектом преступлений в сфере компьютерной информации является общественная безопасность (УК РФ), безопасность в сфере компьютерной информация (УК Туркменистана). Родовым объектом преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (технологий), является безопасность мира и человечества, отношения в сфере экономики, интересы

личности, безопасность государственной власти и другие охраняемые уголовным законодательством блага.

Обязательным (основным или дополнительным) объектом преступлений, предусмотренных главой 28 УК РФ и 33 УК Туркменистана, следует признавать особый сегмент общественной безопасности и безопасности в сфере компьютерной информации - информационную безопасность.

2. С учетом сравнительно-правового контекста исследования предмет преступлений, предусмотренных главой 28 УК РФ и 33 УК Туркменистана, определен как компьютерная информация и (или) национальная критическая информационная инфраструктура.

3. В настоящем исследовании предложено под преступлениями в сфере компьютерной информации понимать общественно опасные деяния, посягающие на общественную (информационную) безопасность и совершаемые с использованием электронно-вычислительных средств в отношении информации, представленной в форме графического, звукового, числового и текстового содержания на различных электронных носителях информации.

Под преступлениями, совершаемыми с использованием информационно-телекоммуникационных сетей (технологий), следует понимать совокупность многообъектных общественно опасных посягательств, запрещенных уголовным законодательством, совершение которых сопряженно с технологической составляющей в форме применения информационно-телекоммуникационных сетей (технологий).

4. Отсутствие легально сформулированных определений компьютерной информации и охраняемой законом информации в уголовном законодательстве Туркменистана приводит к трудностям в процессе квалификации преступлений в сфере компьютерной информации (раздел 13 УК Туркменистана). Это обстоятельство не только существенно усложняет работу правоохранительных органов и судебной системы, но и создает

препятствия для обеспечения правосудия и защиты прав граждан. В связи с этим предлагается применительно к анализируемым по УК Туркменистана преступлениям под компьютерной информацией понимать электронные сведения (текстового, числового, звукового и графического содержания), представленные в символьной форме, содержащиеся на материальных электронно-вычислительных носителях, а также различных информационно-телекоммуникационных сетях связи; под охраняемой законом информацией следует понимать информацию, для которой действующим законодательством Туркменистана установлен особый статус правовой защиты. Вместе с тем особый статус правовой защиты такой информации предусматривает специальные правила ее хранения, обработки и распространения в целях обеспечения ее конфиденциальности. При этом к информации с особым статусом правовой защиты могут относиться любые сведения, подпадающие под действие законодательства Туркменистана, регулирующего отношения, связанные с государственной, корпоративной, семейной, личной тайной. Такой подход позволит устранить существующий пробел в понятийно-категориальном аппарате уголовного законодательства Туркменистана (раздел 13 УК Туркменистана).

5. В диссертации показано, что способами совершения преступлений в сфере компьютерной информации по уголовному законодательству Российской Федерации и Туркменистана (глава 28 УК РФ и глава 33 УК Туркменистана) является септет противоправных манипуляций в информационной системе: 1) незаконный доступ (УК Туркменистана) / неправомерный доступ (УК РФ) – проникновение в электрическую систему устройства, а также информационную систему, в которой содержится информация; 2) принуждение к передаче информации (УК Туркменистана) – умышленное применение физических и моральных форм насилия с целью завладения информацией; 3) уничтожение (УК РФ и УК Туркменистана) – действия, направленные на уничтожение информации; 4)изменение

(формулировка в УК Туркменистана) /модификация (формулировка в УК РФ) – процесс изменения первоначального вида информации путем внесения корректировок; 5) копирование (УК РФ и УК Туркменистана) – операция по созданию дубликата информации; 6) нарушение нормальной работы (такую формулировку предлагает УК Туркменистана) / неправомерное воздействие (такую формулировку предлагает УК РФ, но данные формулировки имеют одно значение) – постороннее вмешательство в деятельность объектов системы информационного обеспечения и информационных сетей; 7) создание/использование/распространение (УК РФ и УК Туркменистана) – последовательный этап разработки программного обеспечения с вредоносным содержанием с целью нарушения работы информационной системы, а также завладения сведениями, представленными в цифровой форме.

6. Диссертантом определено, что средствами совершения преступлений в сфере компьютерной информации и иных преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (технологий), по уголовному законодательству Российской Федерации и Туркменистана являются материальные и нематериальные компоненты окружающей среды, а именно электронно-вычислительные системы, цифровое программное обеспечение, а также средства связи. В связи с этим предложено выделить триаду основных средств совершения данных преступлений: вредоносное программное обеспечение (разновидностями которого могут быть шпионские программы, троянские черви, вирусы, логические бомбы, информационные вредоносные программы и др.); коммуникационные системы связи (в частности, информационно-телекоммуникационные сети); компьютерные устройства (компьютеры, планшеты, промышленные вычислительные машины, суперкомпьютеры, портативные компьютерные устройства и др.).

7. Установлено, что, начиная с 2022 г. в уголовном законодательстве Российской Федерации и Туркменистана существуют заметные различия в подходах к структурированию положений Особенной части уголовного закона

об ответственности за преступления в сфере компьютерной информации. Уголовный кодекс Туркменистана предусматривает отдельный раздел XIII «Преступления в сфере компьютерной информации». В данный раздел включена глава 33, именуемая «Преступления в сфере информатики и связи». В то же время в Уголовном кодексе Российской Федерации указанные посягательства описаны в главе 28 «Преступления в сфере компьютерной информации», которая, в свою очередь, интегрирована в более крупный раздел IX «Преступления против общественной безопасности и общественного порядка». Вместе с тем существенные различия положений главы 33 «Преступления в сфере информатики и связи» УК Туркменистана и главы 28 «Преступления в сфере компьютерной информации» также обусловлены многообразием видов преступных деяний, интегрированных в главу 33 «Преступления в сфере информатики и связи» УК Туркменистана. В УК Туркменистана к специфичным видам противоправных деяний, не имеющим аналогов в УК РФ, относятся: распространение заведомо сфальсифицированной информации; оказание услуг по размещению интернет-ресурсов, преследующих незаконные цели; неправомерное изменение идентификационного кода абонентского устройства сотовой связи; нарушение требований технических измерений беспилотных летающих аппаратов. Вышеуказанные различия в структуре уголовных кодексов отражают не только юридические, но и социально-правовые аспекты, характерные для каждой из упомянутых стран, а также свидетельствуют о различных подходах юридической техники.

8. Аргументирована необходимость корректировки названия главы 33 «Преступления в сфере информатики и связи» и раздела 13 Уголовного кодекса Туркменистана «Преступления в сфере компьютерной информации» с точки зрения правил юридической техники и классификации объектов уголовно-правовой охраны. Предлагается раздел 13 Уголовного кодекса Туркменистана именовать «Преступления в сфере информатики и связи», а

главу 33 «Преступления в сфере компьютерной информации». Согласно информационно-технологическим основаниям сфера информатики и связи охватывает собой область компьютерной информации; равным образом, как категории информации и информатики включают в себя понятие компьютерной информации.

9. В уголовно-правовой науке Российской Федерации и Туркменистана принято преступления в сфере компьютерной информации и иные преступления, совершаемые с использованием информационно-телекоммуникационных сетей (технологий), унифицировать под термином «киберпреступность». Однако на сегодняшний день в уголовно-правовой науке нет единой дефиниции вышеуказанного термина. Исходя из того, что объединяющим фактором преступлений в сфере компьютерной информации и иных преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (технологий), является применение при совершении противоправного деяния технического (компьютерного) средства, рекомендовано в целях унификации в уголовно-правовой науке Российской Федерации и Туркменистана преступления в сфере компьютерной информации и иные преступления, совершаемые с использованием информационно-телекоммуникационных сетей (технологий), именовать более общим понятием «компьютерные преступления», которое также включает в себя преступления, связанные с компьютерной информацией и устройствами, вредоносным программным обеспечением и (или) системами связи (информационно-телекоммуникационными сетями и иными технологиями).

10. В связи с тем, что компьютерные технологии развиваются с высокой скоростью, а компьютерная информация становится все более значимым элементом общественной жизни, возникает необходимость в усилении мер уголовно-правового противодействия соответствующим преступлениям. В диссертации смоделирован новый состав преступления в сфере компьютерной информации, который предлагается описать в статье 274^3 «Неправомерная

модификация программного обеспечения беспилотных систем» УК РФ. Предметом данного преступления следует признать программное обеспечение беспилотных систем, в частности аэромобильных комплексов, аэростатов, коптеров, квадрокоптеров; беспилотных летальных аппаратов самолетного типа; беспилотных систем наземного и морского типов. Объективную сторону данного преступления целесообразно определить, как неправомерную модификацию беспилотных систем, повлекшую за собой угрозу нарушения общественной безопасности и общественного порядка (информационной безопасности). Данный уголовно-правовой запрет позволит более эффективно бороться с нелегальным программированием таких аппаратов, что является одной из актуальных проблем современности.

Также предлагается новый состав преступления в сфере компьютерной информации - статья 272^2 «Принуждение к передаче компьютерной информации» УК РФ. Данная новелла направлена на дополнительную защиту лиц, обладающих разрешительным доступом к охраняемой законом информации.

11. Создание и внедрение программ развития цифровизации в государственную, экономическую и социальную сферы жизни Туркменистана предопределяет совершенствование уголовного законодательства Туркменистана в направлении противодействия преступлениям в сфере цифровых имущественных отношений. В связи с этим в целях обеспечения правопорядка и защиты имущественных (цифровых) прав граждан возникает необходимость в разработке и внедрении новых уголовно-правовых норм. Предлагается ввести в Уголовный кодекс Туркменистана ст. 249^1 «Хищение в сфере цифровых средств». Это дополнение должно предусматривать уголовную ответственность за преступления, связанные с получением незаконной личной выгоды в форме различных видов имущества, включая электронные денежные средства (криптовалюта), другие цифровые имущественные ценности (электронные файлы, цифровые рукописи, ценные

бумаги если они выступают в цифровой форме). Внедрение первой уголовно-правовой нормы в сфере цифровых имущественных отношений в Уголовный кодекс Туркменистана позволит защитить имущественные блага граждан страны.

12. Разработан и направлен в Верховный Суд Туркменистана авторский проект постановления Пленума Верховного Суда Туркменистана «О некоторых вопросах, возникающих у судов при рассмотрении уголовных дел о преступлениях в сфере компьютерной информации» для целей обеспечения единых подходов в области применении уголовного законодательства об ответственности за преступления в сфере компьютерной информации (в целях апробации проект документа направлен в Верховный Суд Туркменистана 3 февраля 2025 года).

Степень достоверности результатов. Достоверность, представленных в диссертации результатов и выводов обоснована применением широкого спектра научной методологии, включающей в себя сравнительно-правовой анализ положений уголовного законодательства Российской Федерации и Туркменистана; теоретико-прикладные положения диссертации основаны на научных изысканиях отечественных и зарубежных ученых-юристов; теоретико-прикладные результаты исследования представлены в ходе выступления на научных конференциях всероссийского и международного уровней, а также путем направления результатов исследования в профильные органы государственной власти Туркменистана.

Апробация результатов исследования. Ключевые научные результаты диссертационного исследования отражены в 10 научных статьях (5 из них – в рецензируемых изданиях ВАК).

Результаты исследования отражены в докладах на международных и всероссийских научно-практических конференциях. Это Международная научно-практическая конференция «Юридическая наука и образование в XXI веке», посвященная 50-летию юридического факультета Самарского

университета (2020 г., Самарский университет); Всероссийская научно-практическая конференция «К 300-летию Российской Прокуратуры: Прокурорский надзор в сфере безопасности на транспорте» (14 мая 2021 г., Самарский университет, Самарская Губернская Дума); Всероссийская научно-практическая конференция «Защита прав органами прокуратуры (к 300-летию российской прокуратуры)» (2022 г., Самарский университет); IV Международная научно-практическая конференция «Право и информация: вопросы теории и практики» (г. Пятигорск, 2022 г.); XIX Международная научно-практическая конференция «Уголовное право: стратегия развития в XXI веке» (г. Москва, 2022 г.); XX Международная научно-практическая конференция «Уголовное право: стратегия развития в XXI веке» (г. Москва, 2023 г.); X Международная научно-практическая конференция «Актуальные проблемы уголовного законодательства на современном этапе (г. Волгоград, 2023 г.); XXIV Международная научно-практическая конференция «Кутафинские чтения» (г. Москва, 2023 г.); II Международная научно-практическая конференция «Актуальные вопросы обеспечения национальной безопасности» (г. Санкт-Петербург, 2023 г.); III Саратовский юридический форум (г. Саратов, 2023 г.); V Международная научно-практическая конференции «Эра человека и машины: историческая динамика государственно-правовых перемен» Университет имени О.Е. Кутафина (МГЮА); Клуб уголовного права «De lege lata»; Всероссийская научно-практическая конференция «Государство и право: вопросы методологии, истории, теории и практики функционирования» (2023 г., Самарский университет); Международная научно-практическая конференция «Современное международное право: проблемы и вызовы» (2023 г., Самарская Губернская Дума); Всероссийская научно-практическая конференция «Кодификация российского законодательства: история, теория, практика» (приуроченная к 160-летию Судебной реформы 1864 года и посвященная 55-летию юридического института Самарского университета)

(2025 г., Дом Правительства Самарской области); Всероссийская научно-практическая конференция «Исторические и правовые уроки Великой Победы: памяти фронтовиков-служителей закона» (2025 г., Самарский университет) и др.

Соискатель ученой степени кандидата юридических наук является лауреатом областного конкурса «Молодой ученый» в 2024 году в номинации «Аспирант» за научно-исследовательскую работу «Сравнительно-правовое исследование преступлений в сфере компьютерной информации по уголовному законодательству Российской Федерации и Туркменистана».

Отдельные положения диссертации были апробированы при ведении практических занятий по дисциплинам «Правозащитная деятельность», «Правовые системы современности» в федеральном государственном автономном образовательном учреждении высшего образования «Самарский национальный исследовательский университет имени академика С.П. Королева».

Структура диссертации обусловлена объектом, предметом, целью и задачами исследования. Диссертация состоит из введения, трех глав, включающих семь параграфов, заключения, списка литературы, приложений.

Глава 1. Социально–правовой анализ преступлений в сфере компьютерной информации и иных преступлений, совершаемых с использованием информационно – телекоммуникационных сетей (технологий)

1.1. Общая характеристика преступлений в сфере компьютерной информации и иных преступлений, совершаемых с использованием информационно – телекоммуникационных сетей (технологий), по уголовному законодательству Российской Федерации

Научно-технический прогресс существенно изменил основные черты преступности. Придал им цифровую виртуальность, а также поспособствовал использованию научно-технологических разработок для совершения этих самых преступлений[1]. Более того, использование высоких технологий увеличили прогрессию латентности таких преступлений, что по своей сути является проблемой для целых государств, в том числе и Российской Федерации.

Научно-технический прогресс принес в повседневную жизнь множество удобных и полезных технических средств, в том числе компьютеры, гаджеты, телефоны, и в конце концов связал все данные устройства между собой информационно-телекоммуникационными сетями, в том числе сетью «Интернет».

Происхождение слова «информация» в русском языке относится к периоду образования Российской Империи, когда в язык проникли множественные заимствования. С.И. Ожегова трактует слово информация - «сведения об окружающем мире и протекающих в нем процессах,

---

[1] См.: Корпеев, А.Г. «О предмете преступлений, совершаемых с использованием информационно-телекоммуникационных сетей, по уголовному законодательству Российской Федерации и Туркменистана». Юридический аналитический журнал. 2023. 18 (1). С. 20-24.

воспринимаемых человеком или специальным устройством»[1]. Сегодня информация является ценным благом, которое охраняется законом от преступных посягательств.

Основная задача государства, как отмечает Попов К.И. и Майоров А.В., выражается в противодействии деструктивным проявления в цифровом пространстве[2].

Но, как можно заметить, с использованием информационных технологий, устройств совершаются не только преступления, посягающие на компьютерную информацию, а также и другие преступления, характеризующиеся как многообъектные. Иными словами, результатом противоправной деятельности человека может стать ущерб не только информации, содержащейся на технических носителях, но и общественным отношениям, которые по своей сути имеют приоритетную уголовно-правовую охрану, а равно защиту государства от противоправных посягательств.

Вообще в законодательной плоскости, а именно согласно ст. 2 Федерального закона от 27.07.2006 № 149 – ФЗ «Об информации, информационных технологиях, защите информации», под термином «информация» следует понимать сведения (сообщения, данные) независимо от формы их представления[3].

Вместе с тем возникает вопрос легального определения компьютерной информации. Тут на сегодняшний день также имеется определённое понимание со стороны законодателя. В ст. 272 Уголовного кодекса Российской Федерации в примечании 1 компьютерная информация определяется как сведения (сообщения, данные), представленные в форме

---

[1] См: Ожегов С.И., Шведова, Н.Ю. Толковый словарь русского языка (А до Я). [Электронный ресурс]. – Режим доступа: https://ozhegov.info/slovar/?q=%D0%98*.

[2] Попов, К.И., Майоров, А. В. Правовые основы противодействия преступлениям в сфере компьютерной информации в сети Интернет // Вестник УрФО. Безопасность в информационной сфере. 2013. № 3 (9). С. 38.

[3] Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 31.12.2014) "Об информации, информационных технология и о защите информации"// СПС «КонсультантПлюс».

электрических сигналов, независимо от средств их хранения, обработки и передачи[1].

С точки зрения информатики словосочетание представленная в форме электрических сигналов» не совсем верно, так как информация в информационном пространстве представлена в форме бинарного кода (в форме символов). Данная система как раз является тем самым маршрутизатором при передаче информации, а также контролирует хранение такой информации на определённом носителе. Простыми словами, информация представляется в виде зашифрованных цифр в общей системе, которая в том числе отвечает и за передачу этой информации между сетями.

Компьютерная информация — это совокупность всех зашифрованных при помощи системы бинарного кода сообщений и данных, образующая информационное пространство, в котором данные хранятся, собираются, обрабатываются и передаются по сетевым каналам. Одним из важных моментов созидания информационного пространства являются рамки его поля действия, в данном случае следует сказать, что информационное пространство может быть реализовано в рамках государства, позволяя тем самым осуществлять хранение, накопление, обрабатывание, а также передачу информации с целью обеспечения функционирования государственной информационной инфраструктуры, а равно обеспечения деятельности государственных органов, частных лиц в использовании информации.

В.Н. Лопатин предлагает под информационной системой понимать «многоуровневую систему, вбирающую в себя информацию, а также технологические элементы, обеспечивающие процесс обработки, хранения и распространение сведений различной формации»[2].

---

[1] Уголовный Кодекс РФ от 13 июня 1996 № 63-ФЗ. [Электронный ресурс]. URL.: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения 22.05.2024).

[2] Лопатин В.Н. Теоретико-правовые проблемы защиты единого информационного пространства и их отражение в системах российского права и законодательства // Труды по интеллектуальной собственности. Т.2. / Гл. редактор Коростелева С. В. – М.: Институт международного права и экономики имени А.С. Грибоедова (ИМПЭ), Кафедра ЮНЕСКО по авторскому праву и другим отраслям права интеллектуальной собственности при участии МГЮА, 2000. С. 55.

С другой стороны, можно говорить и об информационном пространстве мирового масштаба, позволяющем осуществлять взаимодействие посредством хранения, собирания и передачи информации по информационным сетям между государствами, а также иными необходимыми информационными взаимодействиями в информационном поле мира.

Говоря о информационном пространстве, можно отметить, что данная система взаимодействия является ключевым фактором обеспечения цифровизации государственных структур, сфер жизнедеятельности общества и человека. Кроме того, в 2021 году в Российской Федерации издан Указ Президента Российской Федерации «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности», в котором обозначаются государственные задачи в сфере обеспечения интеграционных процессов, в сфере оптимизации обеспечения информационной безопасности путем организации межгосударственного диалога через международные организации[1].

Исходя из вышеизложенного, можем заключить, что компьютерная информация является составным компонентом информационного пространства и по своей сущности генерирует различные общественно-информационные отношения, возникающие при сборе, обработке и передаче любых сведений, включая различные сообщения в любом цифровом виде. Ввиду этого имеется необходимость обеспечения безопасной работы используемых технологий, защиты информационных прав субъектов, использующих компьютерную информацию, и средств, обеспечивающих рекуперацию названной информации. В когорту отношений в сфере защиты информационных прав также входят отношения, связанные с контрафакцией данных прав, фальсификацией, уничтожением, изменением, что по своей сути

---

[1] Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности: Указ Президента РФ от 12 апреля 2021 г. № 213. [Электронный ресурс] URL:http://www.consultant.ru/document/cons_doc_LAW_381999/9bbf31c7586971ae3d3076bfb49080d41d6c4484 (дата обращения: 30.07.2024).

является отправной точкой признания данных прецедентов общественно опасными.

Данные нарушения информационных прав неспроста называют общественно опасными. Исходя из изложенного, следует понимать, что информация, в том числе компьютерная информация, не всегда является удобным средством взаимодействия, придуманным человеком. В данном случае словосочетание «придуманное человеком» дает основания понимать, что алгоритмы работы информационной системы и ее частей в виде компьютерной информации могут быть уязвимыми, что, в свою очередь, может повлечь общественно опасные последствия.

Каждая составляющая информационной безопасности может быть потенциальным объектом деяния, и по данному принципу можно сформировать группу преступлений.

Однако в двух вышесказанных информация является основополагающим звеном, обеспечение целостности которой является приоритетной задачей государства, в этом смысле целостность информации определяется через призму отсутствия любых вмешательств в ее функционирования со стороны третьих лиц, не имеющих на то нормативное право[1].

Рассматривая понятие информационно-телекоммуникационные сети, следует обратиться к Федеральному закону «Об информации, информационных технологиях и о защите информации», в соответствии с которым информационно-телекоммуникационная сеть — это технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники[2].

---

[1] ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. [Электронный ресурс]. URL:https://it-security.admin-smolensk.ru/files/346/50922-2006.pdf (дата обращения: 21.10.2024).

[2] Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 31.12.2014) «Об информации, информационных технология и о защите информации» // СПС «КонсультантПлюс». [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 23.12.2024).

Понятие преступлений в сфере компьютерной информации либо компьютерных преступлений зачастую толкуются очень широко и в принципе является темой для дискуссии. В.Б. Клишков, Е.В. Стебенева, М.А. Яковлев дают следующее определение: «общественно опасное деяние, совершенное в электронной сфере посредством применения информационно-коммуникационных технологий, ресурсов компьютерной информации, т. е. компьютерной системы либо сети, непосредственно – в названной системе либо в сети, либо против названных объектов, посягающее в т. ч. на национальную и мировую безопасность (кибертерроризм и пр.), имущество, имущественные права (кражи, мошенничество в киберпространстве), личную безопасность (кибербуллинг, секстинг, груминг, троллинг и пр.), интеллектуальную собственность (плагиат и киберпиратство) и пр.»[1].

«Также возникают вопросы, связанные с толкованием таких понятий, как «преступления в сфере компьютерной информации» и «компьютерные преступления». В уголовно-правовой науке существуют различные позиции по вопросу категоризации и унификации двух обозначенных понятий. Например, Шибаев Д.В. и Лобачев И.В. определяют их как необъединенные общим смысловым наличием»[2]. Стоит согласиться с авторами, что данные понятия являются разными категориями обозначения общественно опасных явлений, широта смыслового понимания данных понятий также имеет существенное различие.

Сама фраза «в сфере компьютерной информации» подразумевает под собой программы, тексты, пароли, т.е. сведения, содержащиеся в памяти компьютера, иными словами, это лишь капля в море огромного разнообразия информационных технологий, а также технических способов противоправного использования технологических инструментов.

---

[1] Клишков, В.Б., Стебенева, Е.В., Яковлев М.А. Киберпреступность: понятие, признаки, основные направления противодействия // Вестник Нижегородского университета им. Н.И. Лобачевского, 2022, 4. С.111.

[2] Шибаев Д.В. и Лобачев И.В. Содержание понятий «преступление в сфере компьютерной информации» // Российский журнал правовых исследований. 2018 № 4 (17). С.134.

В свою очередь компьютерные преступления имеют более широкую правовую природу и включают в себя использование различных вычислительных средств, в том числе стационарные компьютеры, смартфоны, игровые консоли и т.д. *В переводе с английского слово «компьютер» /computer обозначает «вычислитель» (от лат. computare - считать, вычислять), т.е. это устройство, которое вычисляет различные алгоритмы с помощью определённых программ. В комплекс компьютерных устройств следует включить и компьютерные сети либо информационно-телекоммуникационные сети, т.е. взаимосвязь двух вычислителей, которые обмениваются различными данными по каналам данных сетей или комплексно используют общие ресурсы*[1]. По фактическим обстоятельствам компьютерная сеть является частью вычислительного устройства и служит основным взаимоувязывающим звеном между несколькими вычислительными устройствами.

В этом плане имеет смысл унифицировать преступления в сфере компьютерной информации и все иные преступления, сопряженные с использованием информационных технологий, включая сети, в единую и общую когорту – «компьютерные преступления».

Приоритетным направлением в Российской Федерация является налаживание системы всех сфер обеспечения информационной безопасности. Стратегия развития информационного общества на 2017-2030 годы является фундаментальным документом, закрепляющим принципы обеспечения безопасности в информационном пространстве, в том числе обеспечения безопасного использования информационных систем, включая технологии, используемые жителями России[2].

---

[1] Большая российская энциклопедия. [Электронный ресурс]. URL.: https://bigenc.ru/c/komp-iuter-2f2d51 (дата обращения: 07.04.2025).

[2] Стратегия развития информационного общества в Российской Федерации на 2017 – 2030 годы, утвержденной Указом Президента РФ от 9.05.2017 № 203. [Электронный ресурс]. URL: tps://base.garant.ru/71670570/ (дата обращения: 13.08.2023).

В этом смысле исследование феномена деяний в сфере компьютерной информации, а также иные преступления, совершаемые с использованием информационных технологий, являются прерогативой в сфере обеспечения безопасности общественных отношений, охраняемых уголовным законом.

Важным вопросом в сфере обеспечения информационной безопасности является вопрос классификации таких видов преступлений, которые являются важным фактором на пути дифференциации, а также определения видов наказаний. Социально-правовая сущность таких деяний является по своей природе сложной ввиду особенностей признаков составов таких преступлений. Определенные трудности возникают при определении субъективных и объективных признаков, объема уголовного наказания за совершения таких деяний.

Историзация появления таких составов преступлений в системе уголовного права Российской Федерации берет начало еще с последнего десятилетия 20 века, когда появилась глава 28 «Преступления в сфере компьютерной информации», при этом процесс становления норм права в сфере компьютерной информации происходит на стыке появления многих международных нормативных правовых актов, в частности Европейской конвенции о киберпреступлениях от 23.11.2001 (г. Будапешт)[1]. Данная взаимосвязь является оправданной с точки зрения бланкетности таких норм, которая является фактором отсылки на многие иные источники права, включая международные. Конвенция в своем содержании определяет важную для уголовного права категоризацию, в частности путем классификации рассматриваемых преступлений по группам и содержит понятийный аппарат:

[1] Конвенция о преступности в сфере компьютерной информации от 23 ноября 2001 года ETS № 185 //ЭПС «Система ГАРАНТ». [Электронный ресурс]. URL: http://base.garant.ru/4089723/#ixzz5WwK9w8it (дата обращения: 13.08.2023).

Таблица 1[1].

Группы	Преступления в сфере компьютерной информации	Преступления, сопряженные с использованием информационных технологий
Определения	Противоправные деяния, совершаемые в отношении компьютерной информации.	Особые обстоятельства совершения деяний разнообъектной направленности, в процессе которых применяются информационные технологии
Виды	Копирование, модификация, уничтожение информации	Клевета, доведение до самоубийства, мошенничество

Таким образом, конвенция о киберпреступлениях выделяет двухгруппное деление деяний исходя из предметной составляющей и средств совершения многообъектных деяний[2].

Соглашение о сотрудничестве государств – членов Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий от 28.09.2018 (г. Душанбе)[3], которое является методологическим основанием в сфере унификации подходов к обеспечению информационной безопасности на территории стран СНГ. Соглашение характеризует несколько классификаций компьютерных преступлений,

---

[1] Конвенция о преступности в сфере компьютерной информации от 23 ноября 2001 года ETS № 185 //ЭПС «Система ГАРАНТ». [Электронный ресурс]. URL: http://base.garant.ru/4089723/#ixzz5WwK9w8it (дата обращения: 13.08.2023).

[2] Конвенция о преступности в сфере компьютерной информации от 23 ноября 2001 года ETS № 185 //ЭПС «Система ГАРАНТ». [Электронный ресурс]. URL: http://base.garant.ru/4089723/#ixzz5WwK9w8it (дата обращения: 12.08.2024).

[3] Соглашение о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий от 28 сентября 2018 года. [Электронный ресурс]. URL: http://publication.pravo.gov.ru/Document/View/0001202207180005 (дата обращения: 12.08.2024).

включая аналогичное деление, представленное в Конвенции о киберпреступлениях от 23.11.2001 (г. Будапешт) (см. таблицу 1).

В соответствии с постановлением Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершаемых с использованием электронных или информационно-телекоммуникационных сетей, включая сеть “Интернет”», данные деяния классифицируются как совершаемые: (1) в сфере компьютерной информации; (2) с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»[1].

В этой связи глава 28 «Преступления в сфере компьютерной информации» УК РФ в своей структуре содержит следующие индивидуальные составы преступлений.

Ст. 272 УК РФ «Неправомерный доступ к компьютерной информации». *Объективная сторона данного преступления выражается в неправомерном доступе к охраняемой законом компьютерной информации. В данном контексте правовой нормы под неправомерным доступом понимается воздействие на компьютерную информацию с использованием технических средств извне, а также воздействие лица на компьютерную информацию в связи с имеющимся правом доступа к названной информации*[2]**.** *В данном случае, исходя из ч. 1 ст. 272, под воздействием понимается*

---

[1] Постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет». [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_434573/ (дата обращения: 12.08.2024); См.: Корпеев, А.Г. Классификация преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (технологий), по уголовному законодательству Российской Федерации и Туркменистана // Юридический вестник Самарского университета Juridical Journal of Samara University. 2023. Т.9, № 4. С. 102–107.

[2] Уголовный Кодекс РФ от 13 июня 1996 № 63-ФЗ. [Электронный ресурс]. URL.: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения 22.05.2024).

уничтожение, модификация, т.е. изменение первоначального вида (кода) информации, копирование данной информации[1].

Согласно п.2 постановления Пленума Верховного Суда РФ «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”» от 15 декабря 2022 г. № 37 «*под средством содержания данных сведений, а именно компьютерной информации, следует понимать электронно-вычислительные машины, электронные носители, то есть CD-диски, винчестер (жесткий диск), флеш-накопители*[2]*. Под компьютерными устройствами понимаются электронные устройства, способные выполнять функции по приему, обработке, хранению и передаче информации, закодированной в форме электрических сигналов (персональные компьютеры, включая ноутбуки и планшеты, мобильные телефоны, смартфоны, а также иные электронные устройства, в том числе физические объекты, оснащенные встроенными вычислительными устройствами, средствами и технологиями для сбора и передачи информации, взаимодействия друг с другом или внешней средой без участия человека), произведенные или переделанные промышленным либо кустарным способом»*[3].

Под охраняемой законом информацией, исходя из смысла ч. 1 ст. 272, следует понимать информацию, находящуюся под специальным режимом

---

[1] Уголовный Кодекс РФ от 13 июня 1996 № 63-ФЗ. [Электронный ресурс]. URL.: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения 22.05.2024).

[2] Постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет». [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_434573/. (дата обращения: 21.08.2024).

[3] Постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет». [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_434573/. (дата обращения: 21.08.2024).

защиты[1]. К таким сведениям относится любая информация, которая запрещена к свободному распространению законодательством (в том числе государственная тайна, корпоративная тайна, а также персональные данные лица, находящиеся в цифровом обороте, либо хранящиеся на электронных носителях).

Исходя из логики уголовного закона, объектом данного преступления признаются общественные отношения в сфере различных форм (уничтожение, блокирование, модификация) использования компьютерной информации[2]. Субъектом признается лицо, достигшее 16-летнего возраста (*общий субъект*), однако ч 3. рассматриваемой статьи выделяет специальный субъект преступления, а именно лицо, совершившее преступление с использованием своего служебного положения[3]. Субъективная сторона преступления выражена в форме умысла. В качестве квалифицирующих признаков признаются причинение крупного ущерба или совершение преступления из корыстной заинтересованности, совершение группой лиц по предварительному сговору, причинение тяжких последствий или угроза наступления тяжких последствий[4].

В рамках статьи 272 Уголовного кодекса Российской Федерации, доступ к информации, включая случаи неправомерного доступа, осуществляется без получения предварительного разрешения от владельца этой информации. В данном случае речь идет об отсутствии согласия со стороны лица, имеющего разрешительный доступ к информации.

---

[1] Уголовный Кодекс РФ от 13 июня 1996 № 63-ФЗ. [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_10699/(дата обращения: 5.05.2025).

[2] См.: Прокурор разъясняет (Предусмотрена ли уголовная ответственность за неправомерный доступ к компьютерной информации?). [Электронный ресурс]. URL: https://epp.genproc.gov.ru/ru/web/proc_73/activity/legal-education/explain?item=94089592#/ (дата обращения: 5.05.2025).

[3] Уголовный Кодекс РФ от 13 июня 1996 № 63-ФЗ. [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 5.05.2025).

[4] См.: Прокурор разъясняет (Предусмотрена ли уголовная ответственность за неправомерный доступ к компьютерной информации?). [Электронный ресурс]. URL: https://epp.genproc.gov.ru/ru/web/proc_73/activity/legal-education/explain?item=94089592#/ (дата обращения: 5.05.2025).

Следует отметить, что вышеуказанные способы (уничтожение, блокирование, модификация) на сегодняшний день терминологически остаются не регламентированными. Разночтение и отсутствие единых основ терминологического характера оставляют неясность объективной стороны данного деяния.

Многие авторы высказывают свою позицию по данному вопросу, например, В.В. Хилюта считает, что *модификация является общим знаменателем и объединяет в данном понятии все остальные действия, такие как блокирование, удаление, ввод информации, являющиеся способом воздействия на охраняемую законом информацию*[1].

Ст. 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ». *Объективная сторона преступления выражена в создании, распространении или использовании компьютерных программ либо иной компьютерной информации, а именно в выполнении хотя бы одного действия, указанного ч. 1 данной статьи, а равно в создании, использовании и распространении вредоносных компьютерных программ*[2].

Исходя из статьи 1261 Гражданского кодекса Российской Федерации, под компьютерной программой следует понимать определенный массив данных и командных функций ЭВМ. Вредоносной программой в техническом плане является программа (а именно измененный (искаженный) переносимый код), содержащаяся на внешних и внутренних носителях, которую можно переносить/распространять на иные технические средства, с целью уничтожения, завладения, изменения данных и сведений технического средств[3].

---

[1] Хилюта, В.В. Уголовная ответственность за хищения с использованием компьютерной техники // Журнал российского права. 2014. № 3. С. 117.

[2] Уголовный Кодекс РФ от 13 июня 1996 № 63-ФЗ. [Электронный ресурс]. URL.: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения 22.05.2024).

[3] Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 № 230-ФЗ // Собрание законодательства РФ. № 52.

Субъективная сторона преступления выражена в форме умысла. Субъектом преступления признается физическое лицо, достигшее 16-летнего возраста, также ч. 2 данной статьи обозначается специальный субъект преступления – лицо, совершившее преступление с использованием служебного положения. Квалифицирующие признаки приведены следующим образом: деяние, совершенное группой лиц по предварительному сговору или организованной группой, причинившее крупный ущерб; под крупным ущербом понимается ущерб в размере больше одного миллиона рублей; а также деяние, повлекшее тяжкие последствия или создавшее угрозу наступления таких последствий[1].

Ст. 274 УК. «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей». Объективная сторона преступления выражена в нарушении правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей, а также правил доступа к информационно-телекоммуникационным сетям[2].

На практике это означает, что любые операции, проводимые с использованием технологических устройств и систем должны быть осуществлены на основе протокола безопасности, регламентирующего работу информационной системы. Нарушение протокола безопасности приводит к тяжким последствиям: нарушение нормального функционирования информационных систем, нарушения целостности данных и прочих негативных последствий.

Согласно ч. 1 статьи 274^1 объективная сторона преступления характеризуется созданием, распространением и использованием

---

[1] Уголовный Кодекс РФ от 13 июня 1996 № 63-ФЗ. [Электронный ресурс]. URL.: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения 22.05.2024).

[2] Уголовный Кодекс РФ от 13 июня 1996 № 63-ФЗ. [Электронный ресурс]. URL.: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения 22.05.2024).

компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации[1].

Исходя из ч. 2 ст. 274[1], объективная сторона преступления характеризуется неправомерным доступом к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре, в том числе с использованием компьютерных программ либо иной компьютерной информации, которые заведомо предназначены для неправомерного воздействия на критическую информационную инфраструктуру[2].

В части 3 статьи 274[1] объективная сторона характеризуется нарушением правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, или информационных систем, автоматизированных систем управления, сетей электросвязи[3].

Субъектом данных деяний является лицо, достигшее 16–летнего возраста на момент совершения преступления, иными словами, общий субъект, вместе с тем деяние может быть совершенно специальным субъектом преступления, т.е. лицом с использованием своего служебного положения[4].

Ст. 274[2] «Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети

---

[1] Уголовный Кодекс РФ от 13 июня 1996 № 63-ФЗ. [Электронный ресурс]. URL.: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения 22.05.2024).

[2] Уголовный Кодекс РФ от 13 июня 1996 № 63-ФЗ. [Электронный ресурс]. URL.: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения 27.05.2024).

[3] Уголовный Кодекс РФ от 13 июня 1996 № 63-ФЗ. [Электронный ресурс]. URL.: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения 22.05.2024).

[4] Ефремова, М.А. Уголовно-правовая охрана информационной безопасности: дисс. … док. юрид. наук: 12.00.08. М. 2017. С. 362.

«Интернет» и сети связи общего пользования». *Согласно части 1 статьи 274[2] объективная сторона преступления характеризуется нарушением порядка установки, эксплуатации и модернизации в сети связи технических средств противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации*[1].

В части статьи 274[2] объективная сторона деяния выражается в нарушении требований к пропуску трафика через технические средства противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет»[2].

Также в рамках уголовного законодательства Российской Федерации присутствует целый ряд нормативных актов, которые регламентируют и определяют специфические виды преступлений, сопряженные с применением информационно-телекоммуникационных технологий.

В уголовном – правовой науке под преступлениями в сфере информационно-телекоммуникационных технологий понимают «запрещенные уголовным законом общественно опасные деяния, посягающие на общественные отношения, обеспечивающие безопасность процессов и методов поиска, сбора, хранения, обработки, предоставления, распространения информации посредством средств вычислительной техники и информационно-телекоммуникационных сетей»[3].

Согласно принятой по инициативе Российской Федерации в 2024 году Конвенции ООН о киберпреступности под информационно-телекоммуникационной системой понимается «любое устройство или группу соединенных или взаимосвязанных устройств, одно или несколько из которых

---

[1] Уголовный Кодекс РФ от 13 июня 1996 № 63-ФЗ. [Электронный ресурс]. URL.: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения 22.05.2024).

[2] Уголовный Кодекс РФ от 13 июня 1996 № 63-ФЗ. [Электронный ресурс]. URL.: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения 22.05.2024).

[3] Ефремова, М.А. Уголовно-правовая охрана информационной безопасности: дисс. … док. юрид. наук: 12.00.08. М. 2017. С.15.

по команде программы производит сбор, хранение и автоматическую обработку электронных данных»[1].

Несомненно, использование информационных технологий является элементом «facile modo», что означает использование легкого пути совершения противоправного деяния, а также приводит правоприменителей в тупик ввиду особенностей - анонимного характера совершения таких деяний и зачастую преобладания экстерриториального характера подобных преступлений.

«В связи с этим законодатели Российской Федерации, понимая всю опасность противоправного использования информационно-телекоммуникационных сетей (технологий), дифференцируют уголовную ответственность в имеющихся составах преступлений, объектами которых могут являться жизнь и здоровье личности (пп. «д» ч. 2 ст. 110, пп. «д» ч. 3 ст. 110^1 УК РФ,), общественная безопасность (ч. 2 ст. 205^2 УК РФ, пп. «в» ч.3 ст. 222 УК РФ, пп. «б» ч.2 ст. 228^1 УК РФ, пп. «г» ч. 2 ст. 245 УК РФ, пп. «б» ч.2 ст. 258^1 УК РФ,), порядок в сфере экономической деятельности (ч. 1 ст. 171^2 УК РФ), собственность (ч. 1 ст. 159^6 УК РФ)»[2].

Е.А. Русскевич справедливо отметил: «Современное состояние преступности со всей очевидностью указывает на то, что многие посягательства на традиционно охраняемые уголовным законом общественные отношения «сращиваются» с преступлениями в сфере компьютерной информации. Так, в настоящее время такая тенденция отчетливо прослеживается по делам о нарушении неприкосновенности частной жизни (ст. 137 УК РФ), нарушении тайны переписки, телефонных

---

[1] Конвенция против киберпреступности; Укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям, принята резолюцией 79/243 Генеральной Ассамблеей от 24 декабря 2024 года. [Электронный документ].URL: https://www.un.org/ru/documents/treaty/A-RES-79-243 (дата обращения: 14.05.2025).

[2] См.: Корпеев А. Г. Классификация преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (технологий), по уголовному законодательству Российской Федерации и Туркменистана // Юридический вестник Самарского университета Juridical Journal of Samara University. 2023. Т.9, № 4. С. 102–107.

переговоров, почтовых, телеграфных или иных сообщений (ст. 138 УК РФ), нарушении авторских и смежных прав (ст. 146 УК РФ) и др. В каждом таком случае правоприменитель прибегает к вменению совокупности преступлений, дополнительно квалифицируя действия субъекта по ст. 272 УК РФ. Вместе с тем неправомерный доступ к охраняемой законом компьютерной информации стал настолько типичным для определенного круга традиционных составов преступлений, что имеются все основания для конкретизации этих компьютеризированных форм непосредственно в соответствующих статьях Особенной части УК РФ»[1].

Информационно-телекоммуникационная сеть (ИТС) является сложноустроенной системой современной инфраструктуры связи и обмена информацией[2].

В связи со спецификой использования цифровых средств основным вопросом при квалификации данных преступлений является место совершения преступления. Согласно названному Постановлению Пленума от 15.12.2024 № 37 *местом совершения преступлений, совершаемых с использованием компьютерных средств и средств связи признается локация, с которой преступником совершаются противоправные действия.*[3].

Следует выделить два признака, характеризующих место совершения преступлений:

1. *Территориальный признак.*

---

[1] Русскевич Е.А. Уголовное право и «цифровая преступность»: проблемы и решения: монография. 2-е изд., перераб. и доп. – М.: ИНФРА-М, 2022. С. 107

[2] См.: Овсюков, Д.А. Корыстные преступления против собственности с использованием информационно-телекоммуникационных сетей: вопросы квалификации: Дис. … канд. юрид. наук: 5.1.4/ Д.А. Овсюков. – Москва, 2022. – 231 с.

[3] Постановление Пленума Верховного Суда РФ от 15.12.2022 N 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет». [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_434573/. (дата обращения: 21.08.2024).

Если преступник физически находится в стране, в которой совершается преступление, то это место может быть рассмотрено как место совершения названных преступлений[1].

2. Экстерриториальный признак.

Совершение преступления из различных точек мира[2].

В связи со спецификой совершения названных преступлений следует учитывать широкий спектр факторов при определении места совершения, и оно может быть, как физическим, так и виртуальным пространством, где преступник осуществляет незаконные действия или где в результате преступления причиняется ущерб.

Важно отметить, что 64,8 % опрошенных респондентов считает местом совершения преступлений в сфере компьютерной информации, считают место наступления последствий, входящих в объективную сторону преступлений[3].

Кроме того, при квалификации таких деяний следует установить вид технического средства, приименного при совершении общественно опасного действия[4].

Преступления сфере компьютерной информации и иные преступлений, совершаемые с использование информационных технологий, обычно определяют различным понятийно-категориальным рядом, например, «компьютерные преступления, «компьютеризованные деяния»[5].

---

[1] См.: Овсюков, Д.А. Корыстные преступления против собственности с использованием информационно-телекоммуникационных сетей: вопросы квалификации: Дис. … канд. юрид. наук: 5.1.4/ Д.А. Овсюков. – Москва, 2022. С. 151.

[2] См.: Там же.

[3] Результаты опроса в Приложении 1 к диссертации.

[4] Русскевич Е.А. Уголовное право и «цифровая преступность»: проблемы и решения: монография. 2-е изд., перераб. и доп. – М.: ИНФРА-М, 2022. С 242.

[5] См. например: Лукинский И.С., Баулина А.А. О перспективных направлениях сотрудничества министерства внутренних дел государств – участников СНГ в сфере противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий // Противодействие преступлениям в сфере информационно-телекоммуникационных технологий: сборник научных трудов международной научно-практической конференции. М., 2024. С. 557-561; Противодействие преступлениям, совершаемым в сфере информационных технологий (учебник) (коллектив авторов; под науч. ред. И.А. Калиниченко). - "ИНФРА-М", 2023. - 642 с.

Согласно концепции территориального охвата, Д.А. Овсюков рассматривает информационные технологии следующим образом: выделяя локальные сети, которые имеют ограниченный охват территории (в данном случае это может быть офис, здание, в которых взаимоувязаны абоненты), региональные (в данном случае это город, поселение, область либо район) и глобальные, которые охватывают и объединяют уже страны, а равно предназначены для длинных расстояний[1].

Огромное число видов компьютерных преступлений являются глобальной проблемой на пути к противодействию им, однако из широкого массива следует выделить компьютерное мошенничество и распространение вредоносных программ[2]: об этом свидетельствуют отчеты в сфере безопасности информационно-телекоммуникационных технологий[3].

Вместе с тем на сегодняшний день в целях совершения противоправных деяний активно используются беспилотные системы. Которые можно классифицировать исходя из стихии применения: воздушные, морские, наземные. В связи с участившимися случаями активного использования таких систем мы предлагаем предлагается добавить статью 274[3] «Неправомерная модификация программного обеспечения беспилотных систем». Предметом данного преступления целесообразно признать беспилотные системы, в частности аэромобильные комплексы, аэростаты, коптеры, квадрокоптеры, беспилотные летальные аппараты самолетного типа, монофункциональные беспилотные катера и иные средства беспилотных систем. Объективной стороной данного преступления следует определить неправомерную модификацию беспилотных систем, повлекшую за собой

---

[1] См.: Овсюков, Д.А. Корыстные преступления против собственности с использованием информационно-телекоммуникационных сетей: вопросы квалификации: Дис. … канд. юрид. наук: 5.1.4/ Д.А. Овсюков. – Москва, 2022. С. 24-25.

[2] Cybercriminals’ favourite VPN taken down in global action. [Электронный ресурс]. URL: https://www.europol.europa.eu/newsroom/news/cybercriminals%E2%80%99- favourite-vpn-taken-down-in-global-action (дата обращения: 14.05.2025).

[3] Agari H. Email Fraud Report. 2020. [Электронный ресурс]. URL: https:// www.agari.com/cyberintelligence-research/e-books/agari-h22020-email-fraud-report.pdf (дата обращения: 14.05.2025).

угрозу нарушения общественного порядка, а также тяжкие последствия. Помимо этого, предлагается ввести статью 272^2 УК РФ, которая касается принуждения к передаче компьютерной информации. Данное изменение будет направлено на дополнительную защиту лиц, обладающих доступом к охраняемой законом информации и находящихся под угрозой использования насилия или угроз, связанных с другими ценными для этих лиц благами.

В главе 28 УК РФ на сегодняшний день сформировалась основательная группа преступлений в сфере компьютерной информации, однако процесс научно-технологического развития требует выработки законодательных решений в сфере расширения видов преступлений в сфере компьютерной информации.

1.2. Общая характеристика преступлений в сфере компьютерной информации и иных преступлений, совершаемых с использованием информационно – телекоммуникационных сетей (технологий), по уголовному законодательству Туркменистана

«Для современного Туркменистана, принадлежащего к континентальной правовой семье, основным источником права выступает закон (нормативный правовой акт). Статья 8 Конституции Туркменистана устанавливает в стране верховенство закона. Государство, все его органы и должностные лица связываются правом и конституционным строем»[1].

Нормативным правовым актом, регулирующим общественные отношения уголовно-правового характера в сфере компьютерной информации и информационно-телекоммуникационных сетей, является Уголовный кодекс Туркменистана, который выступает в качестве основополагающего

[1] Аминов, И.И. Правовая система Туркмении «генезис и эволюция»: дис. …док.юрид. наук: 5.1.1. МГИМО, Москва, 2023. С 221.

нормативного правового акта, определяющего правовые рамки для всех участников общественных отношений в данной сфере.

Вместе с тем в Туркменистане в 2022 г. была одобрена Государственная программа, которая направлена на достижение высокого уровня кибербезопасности в стране. Эта программа предполагает комплексный подход к решению задач, связанных с обеспечением защиты информационных ресурсов и систем, и охватывает период с 2022 по 2025 гг., что предполагает долгосрочные меры по повышению уровня защищенности информационной инфраструктуры. Также в Туркменистане действует Постановление Президента Туркменистана об обеспечении кибербезопасности, подписанное 19 января 2024 г. Однако комплекс принятых мер не отражает решение вопросов уголовно-правового характера. В данных документах не раскрываются основные принципы, понятия, которыми следует руководствоваться при противодействии таким преступлениям.

Необходимо подчеркнуть, что в Уголовном кодексе Туркменистана, а также в других нормативных правовых актах страны существует определенный пробел, который касается отсутствия четкого терминологического аппарата, например, отсутствуют определения компьютерная информация и компьютерная безопасность.

Под компьютерной информацией в составах преступлений, предусмотренных статьями 373, 374, 375, 377 УК Туркменистана, следует понимать электронную информацию (имеющую вид текстового, числового, звукового и графического содержания), представленную в символьной форме, содержащуюся на материальных электронно-вычислительных носителях, а также различных информационно-телекоммуникационных сетях связи.

Электронно-вычислительными носителями являются устройства, предназначенные для автоматической обработки и передачи информации, в том числе персональные компьютеры, промышленные компьютеры, смартфоны, портативные игровые приставки, суперкомпьютеры; носители

информации в форме полупроводниковых устройств, в том числе флеш-карты, диски ssd; оптические устройства, в том числе диски DVD, CD, Blu-ray; магнитные устройства, в том числе жесткие диски, дискеты, а также иные информационные устройства.

В рамках существующих законодательных реалий до 2022 г. прослеживалось определённое сходство уголовных кодексов Российской Федерации и Туркменистана в части структурных особенностей преступлений в сфере компьютерной информации.

Однако в 2022 г. Уголовный кодекс Туркменистана в отличие от Уголовного кодекса Российской Федерации претерпел существенных изменений в части установления уголовной ответственности за преступления в сфере компьютерной информации. В 2022 г. был выделен раздел «Преступления в сфере компьютерной информации», в разделе выделена глава «Преступления против информатики и связи», что в свою очередь является по своей сути нарушением приемов юридической техники, в том смысле, что информатика – это не благо, а наука, которая включает в себя в том числе изучение приёмов передачи компьютерной информации[1]. Вместе с тем выделение отдельного раздела и главы для таких преступлений сопутствовало внесению различных видов составов информационных преступлений, которым нет аналогов в Уголовном кодексе Российской Федерации[2].

Однако хочется заметить, что в названии раздела и главы допущены юридико-технические неточности, связанны они в первую очередь с тем, что информатика – это обширный раздел научных знаний, который в том числе включает в себя изучения вопросов компьютерной информации. В этом смысле следовало бы названия раздела и главы поменять места для

---

[1] Данную позицию поддержали 84,5% опрошенных практических работников.

[2] См.: Корпеев, А. Г. Классификация преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (технологий), по уголовному законодательству Российской Федерации и Туркменистана // Юридический вестник Самарского университета Juridical Journal of Samara University. 2023. Т.9, № 4. С. 102–107.

предотвращения неточностей при установлении объективных признаков (объекта).

В рамках текущего обсуждения, опираясь на законодательные основы, которые устанавливаются уголовным законодательством Туркменистана, стоит отметить, что существующие преступные деяния могут быть классифицированы по двум различным типам составов. Эти типы включают в себя специальные преступления в сфере компьютерной информации) и общеуголовные составы (преступления, совершаемые с использованием информационно-телекоммуникационных сетей (технологий), которые, в свою очередь, отражают более общие и распространенные формы преступной деятельности[1].

На сегодняшний день Уголовным кодексом предусмотрены следующие составы в сфере компьютерной информации.

Статья 373 вышеуказанной главы обозначена следующим образом: **«Незаконный доступ к информации, в информационную систему или информационно-телекоммуникационную сеть».** *Объектом данного деяния выступает информационная система, электронная информация, информационно-телекоммуникационная сеть, информационно-коммуникационная инфраструктура*[2]*. Согласно ч. 3 ст. 373 выделяются следующие квалифицирующие признаки: неосторожность, повлекшая за собой тяжкие последствия, деяния, совершенные группой лиц по предварительному сговору или организованной группой. Субъектом преступления является физическое лицо, достигшее 16–летнего возраста. Объективная сторона выражается в форме действия. Субъективная сторона выражается в форме умысла и неосторожности*[3].

---

[1] См.: Иванова, Л.В. Виды киберпреступлений по российскому уголовному законодательству // Юридические исследования. 2019. С. 31.

[2] Уголовный Кодекс Туркменистана от 12 июня 1997 № 222-I. [Электронный ресурс]. URL: online.zakon.kz/Document/? Doc_id=3129586 (дата обращения: 21.07.2024).

[3] Уголовный Кодекс Туркменистана от 12 июня 1997 № 222-I. [Электронный ресурс]. URL: online.zakon.kz/Document/? Doc_id=3129586 (дата обращения: 21.07.2024).

Согласно Закону Туркменистана «Об информации и ее защите» от 3 мая 2014 г. № 72-V *под информационной системой понимается «совокупность в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств. Под информационно-телекоммуникационной сетью понимается технологическая система, предназначенная для передачи по линии связи информации, доступ к которой осуществляется с использованием средств вычислительной техники»*[1].

Ст. 374 «Принуждение к передаче информации». *Объектом данного деяния являются интересы потерпевшего или его близких. Объективная сторона деяния выражена в принуждении к передаче охраняемой законом информации под угрозой применения насилия, либо распространения сведений, позорящих потерпевшего или его близких, а равно в форме действия*[2]*. Субъективная сторона характеризуется в форме умысла. Субъектом преступления является физическое лицо, достигшее 16–летнего возраста. Квалифицирующими признаками являются: рецидив, совершение преступления группой лиц по предварительному сговору, совершение преступления с целью получения информации из информационных систем критически важных объектов информационно-коммуникационной инфраструктуры, совершение преступления организованной группой лиц или преступным сообществом, деяния, повлекшие тяжкие последствия*[3]*. В данном контексте под принуждением к передаче информации следует понимать использование физического или психологического давления с целью вынудить кого-либо к раскрытию личных данных или иных сведений*[4].

---

[1] Закон Туркменистана «Об информации и ее защите» от 3.05.2014 года № 72V. [Электронный ресурс]. URL: https://online.zakon.kz/Document/?doc_id=34731231 (дата обращения: 23.01.2024).

[2] Уголовный Кодекс Туркменистана от 12 июня 1997 № 222-I. [Электронный ресурс]. URL: online.zakon.kz/Document/? Doc_id=3129586 (дата обращения: 21.07.2024).

[3] См.: Корпеев, А.Г. О квалифицирующих признаках преступлений в сфере компьютерной информации по уголовному законодательству России и Туркменистана // Вестник ТГУПБП. 2024. №1. С. 29-36; Уголовный Кодекс Туркменистана от 12 июня 1997 № 222-I. [Электронный ресурс]. URL: online.zakon.kz/Document/? Doc_id=3129586 (дата обращения: 21.07.2024).

[4] Уголовный Кодекс Туркменистана от 12 июня 1997 № 222-I. [Электронный ресурс]. URL: online.zakon.kz/Document/? Doc_id=3129586 (дата обращения: 21.07.2024).

Исходя из анализа контекста статьи 374 УК Туркменистана, мы приходим к выводу, что в названии статьи 374 УК Туркменистана существуют определенные юридические неточности, которые, по нашему мнению, требуют корректировки. В частности, мы считаем, что необходимо уточнить понятийную часть статьи, в частности под принуждением к передаче информации следует подразумевать не просто информацию, а именно «компьютерную информацию».

Ст. 375 «Незаконное уничтожение информации или изменение ее формата». *Объектом данного деяния является охраняемая законом информация и права и законные интересы физических лиц, интересы общества и государства. Объективная сторона деяния выражена в незаконном умышленном уничтожении или изменении формата охраняемой законом информации в информационной системе или проходящей через информационно-телекоммуникационную сеть, хранящейся на электронном носителе, а равно введение в информационную систему заведомо недостоверной информации, если эти деяния повлекли существенное нарушение прав и законных интересов физических и юридических лиц, охраняемых законом интересов общества и государства, а равно в форме действия*[1]*. Субъективная сторона деяния характеризуется в форме умысла. Субъектом преступления является физическое лицо, достигшее 16–летнего возраста. В статье предусмотрены следующие квалифицирующие признаки: деяние, повлекшее тяжкие последствия, совершение преступления группой лиц по предварительному сговору*[2]*.*

Под незаконным уничтожением информации понимается такой процесс, при котором информация в цифровом воплощении, будь то

---

[1] См.: Корпеев, А.Г. О квалифицирующих признаках преступлений в сфере компьютерной информации по уголовному законодательству России и Туркменистана // Вестник ТГУПБП. 2024. №1. С. 29-36; Уголовный Кодекс Туркменистана от 12 июня 1997 № 222-I. [Электронный ресурс]. URL: online.zakon.kz/Document/? Doc_id=3129586 (дата обращения: 21.07.2024).

[2] Уголовный Кодекс Туркменистана от 12 июня 1997 № 222-I. [Электронный ресурс]. URL: online.zakon.kz/Document/? Doc_id=3129586 (дата обращения: 21.07.2024).

различного рода документы, файлы или иные данные информационного характера, подвергаются уничтожению без разрешения владельца или без наличия законных оснований для таких действий. К тому же, к незаконному уничтожению информации также можно отнести и изменение ее формата, когда информация, находящаяся в определенном виде или структуре, подвергается модификации без согласия ее владельца или без уполномоченных оснований. Такие действия могут привести к потере доступности информации, ее корректности или целостности.

Аналогично, как и в статье 374 УК Туркменистана в статью 375 Уголовного кодекса Туркменистана, которая носит название «**Незаконное уничтожение информации или изменение ее формата»**[1], стоит внести определенные уточнения, которые касаются самого названия данной статьи. Важно подчеркнуть, что речь идет о компьютерной информации, которая может быть уничтожена или подвергнута изменениям[2].

Ст. 376 «Нарушение нормальной работы информационной системы и информационно-телекоммуникационной сети». *Объектом деяния является информационная система и информационно-телекоммуникационные сети. Объективная сторона выражается в действии, направленном на нарушение нормальной работы информационной системы и информационно-телекоммуникационных сетей. Субъективная сторона выражается в форме умысла. Субъектом преступления является физическое лицо, достигшее 16–летнего возраста. В статье предусмотрены следующие квалифицирующие признаки: деяние, повлекшее тяжкие последствия или совершенное организованной группой*[3].

---

[1] Уголовный Кодекс Туркменистана от 12 июня 1997 № 222-I. [Электронный ресурс]. URL: online.zakon.kz/Document/? Doc_id=3129586 (дата обращения: 21.07.2024).
[2] Уголовный Кодекс Туркменистана от 12 июня 1997 № 222-I. [Электронный ресурс]. URL: online.zakon.kz/Document/? Doc_id=3129586 (дата обращения: 21.07.2024).
[3] Уголовный Кодекс Туркменистана от 12 июня 1997 № 222-I. [Электронный ресурс]. URL: online.zakon.kz/Document/? Doc_id=3129586 (дата обращения: 21.07.2024).

Ст. 377 «Незаконное присвоение информации». *Объектом деяния является охраняемые законом информация и интересы общества и государства. Объективная сторона преступления выражается в форме действия, направленного на незаконное копирование или присвоение иными способами информации. Субъективная сторона выражается в форме умысла. Субъектом преступления является физическое лицо, достигшее 16–летнего возраста. В статье предусмотрены следующие квалифицирующие признаки: деяние, повлекшее тяжкие последствия или совершенное организованной группой. Незаконное присвоение информации в основном означает незаконное изъятие, копирование или передачу конфиденциальной информации без согласия её владельца*[1].

Незаконное присвоение информации является деянием, которое может привести к последствиям (ущербу) имущественного характера, а также к нарушению прав личности и общественно опасным последствиям. Обычно целью злоумышленников становится информация, касающаяся персональных данных личности, являющаяся корпоративной либо государственной тайной[2].

Ст. 378 «Распространение заведомо сфальсифицированной информации». *Объектом деяния являются охраняемые законом интересы общества и государства. Объективная сторона характеризуется как действие, направленное на распространение заведомо сфальсифицированной информации, повлекшее за собой нарушение прав и интересов физических и юридических лиц. Субъективная сторона деяния выражается в форме умысла. Субъектом преступления является физическое лицо, достигшее 16–летнего возраста. Квалифицирующие признаки: деяние, повлекшее ущерб в крупном размере, деяние, совершенное при проведении массовых мероприятий*

---

[1] Уголовный Кодекс Туркменистана от 12 июня 1997 № 222-I. [Электронный ресурс]. URL: online.zakon.kz/Document/? Doc_id=3129586 (дата обращения: 21.07.2024).

[2] Уголовный Кодекс Туркменистана от 12 июня 1997 № 222-I. [Электронный ресурс]. URL: online.zakon.kz/Document/? Doc_id=3129586 (дата обращения: 21.07.2024).

организованной группой лиц в условиях режима чрезвычайного или военного положения[1].

Ст. 379 «Создание, использование и распространение вредоносных программ». *Объектом деяния является уничтожение, блокирование, изменение формата, распространение охраняемой законом информации. Объективная сторона характеризуется как действие, направленное на незаконное уничтожение охраняемой законом информации. Субъективная сторона деяния выражается в форме умысла. Субъектом преступления является физическое лицо, достигшее 16–летнего возраста. Квалифицирующий признак - деяние, совершенное группой лиц по предварительному сговору или организованной группой*[2].

Ст. 380 «Незаконное распространение электронных источников информации с ограниченным разрешением». *Объектом данного деяния является охраняемая законом информация, содержащая в себе в том числе личные сведения граждан. Объективная сторона характеризуется как действие, направленное на Незаконное распространение информации, на которую законодательством Туркменистана наложены разрешительные ограничения, владельцем или владеющим лицом. Субъективная сторона выражается в форме умысла. Субъектом преступления является физическое лицо, достигшее 16–летнего возраста. Квалифицирующие признаки: деяние, совершенное с использование служебного положения, деяние, повлекшее тяжкие последствия или совершенное по предварительному сговору группой лиц или организованной группой*[3].

Ст. 381 «Оказание услуг по размещению интернет-ресурсов, преследующих незаконные цели». *Объектом данного деяния являются*

---

[1] Уголовный Кодекс Туркменистана от 12 июня 1997 № 222-I. [Электронный ресурс]. URL: online.zakon.kz/Document/? Doc_id=3129586 (дата обращения: 21.07.2024).
[2] Уголовный Кодекс Туркменистана от 12 июня 1997 № 222-I. [Электронный ресурс]. URL: online.zakon.kz/Document/? Doc_id=3129586 (дата обращения: 21.07.2024).
[3] Уголовный Кодекс Туркменистана от 12 июня 1997 № 222-I. [Электронный ресурс]. URL: online.zakon.kz/Document/? Doc_id=3129586 (дата обращения: 21.07.2024).

отношения в сфере оказания услуг в области программного обеспечении технических программ. Объективная сторона деяния характеризуется в форме действия, направленного на размещение интернет-ресурсов, преследующих незаконные цели, а равно оказание незаконных услуг. Субъективная сторона выражается в форме умысла. Субъектом преступления является физическое лицо, достигшее 16–летнего возраста. Квалифицирующий признак - деяние, совершенное по предварительному сговору группой лиц или организованной группой[1].

Ст. 382 «Неправомерное изменение идентификационного кода абонентского устройства сотовой связи, устройства идентификации абонента, а также создание, использование, распространение программ для изменения идентификационного кода абонентского устройства». *Объектом деяния является идентификационный код абонентского устройства. Объективная сторона деяния характеризуется в форме действия, направленного на неправомерное, без согласия производителя или законного владельца изменение идентификационного кода абонентского устройства сотовой связи или создание дубликата карты идентификации абонента сотовой связи. Субъективная сторона выражается в форме умысла. Субъектом преступления является физическое лицо, достигшее 16–летнего возраста. Квалифицирующий признак - деяние, совершенное организованной группой*[2].

Ст. 383. «Умышленное нарушение требований технических измерений беспилотных летающих аппаратов». *Объектом деяния являются отношения, складывающиеся в сфере использования беспилотных летательных аппаратов. Объективная сторона деяния характеризуется как действие, направленное на умышленное нарушение требований технических*

---

[1] Уголовный Кодекс Туркменистана от 12 июня 1997 № 222-I. [Электронный ресурс]. URL: online.zakon.kz/Document/? Doc_id=3129586 (дата обращения: 21.07.2024).

[2] Уголовный Кодекс Туркменистана от 12 июня 1997 № 222-I. [Электронный ресурс]. URL: online.zakon.kz/Document/? Doc_id=3129586 (дата обращения: 21.07.2024).

измерений, определённых нормативными правовыми актами Туркменистана, путём увеличения технических возможностей беспилотных летающих аппаратов. Субъективная сторона выражается в форме умысла. Субъектом преступления является физическое лицо, достигшее 16–летнего возраста[1].

Как мы можем заметить, законодатель Туркменистана пошел по пути приведения систематизационного порядка в расположение уголовно-правовых норм, регулирующих отношения не только в сфере компьютерной информации, но отношения в сфере информатики и связи. Глава, закрепляющая составы преступлений в сфере компьютерной информации, помимо незаконного доступа к охраняемой законом информации выделяет в том числе использование этой информации против интересов общества и государства, образуя при этом важную составляющую регламентации использования, передачи, копирования информации в рамках государства. Основной акцент в данной группе преступлений сделан на регулировании использования различных технических средств, являющихся в том числе инструментом создания неблагоприятной обстановки в государстве. Важным является охват большого количества цифровых устройств, построенных на алгоритмах, которые можно изменять в незаконных целях, например, идентификационный код беспилотного летательного аппарата.

По нашему мнению, спектр понимания информации довольно широк: да, она может быть государственной важности и тогда посягательство на нее приводит к противоправным последствиям, может быть служебной, и в таком случае посягательство на нее наносит ущерб организации, предприятию, но, помимо всего, информация может быть личной, например, сообщения в социальных сетях, заметки в телефоне, научные и литературные работы, содержащиеся на цифровых носителях.

---

[1] Уголовный Кодекс Туркменистана от 12 июня 1997 № 222-I. [Электронный ресурс]. URL: online.zakon.kz/Document/? Doc_id=3129586 (дата обращения: 21.07.2024).

В связи с этим важным моментом является выработка достоверного понятийного аппарата, который играет важную роль при квалификации преступления. По нашему мнению, если законодатель Туркменистана понимает под информацией «все сведения или сообщения в бумажном, электронном или ином виде», то следовало бы исключить словосочетание «охраняемая законом», содержащееся в составах преступлений раздела «Преступления в сфере информатики и связи», ведь исходя из определения, четких критериев этой информации нет. Либо стоит закрепить виды такой информации в части внесения дополнения в термин.

С одной стороны, широкий спектр понимания термина «информация» предоставляет право правоохранительным органам, следственным органам, суду индивидуально устанавливать, является ли информация ценной, нанесен ли ущерб при посягательстве на информацию. С другой стороны, четко выделенные виды информации, воздействие на которые являются противоправным, исключит возникновение лишних вопросов на стадии возбуждения уголовного дела.

Исходя из изложенного, предлагаем под охраняемой законом информацией в статьях главы 33 Уголовного кодекса Туркменистана «Преступления в сфере компьютерной информации» понимать информацию, для которой действующим законодательством Туркменистана установлен особый статус правовой защиты. Вместе с тем особый статус правовой защиты такой информации предусматривает специальные правила ее хранения, обработки и распространения в целях обеспечения ее конфиденциальности. При этом к информации с особым статусом правовой защиты могут относиться любые сведения, подпадающие под действие законодательства Туркменистана, регулирующего отношения, связанные с государственной, корпоративной, семейной, личной тайной. Такой подход позволит устранить существующий пробел в понятийно-категориальном аппарате уголовного законодательства Туркменистана (раздел 13 УК Туркменистана).

Кроме того, в Уголовном кодексе Туркменистана по аналогии с Уголовным кодексом Российской Федерации закреплены составы, сопряженные с использованием информационных технологий в качестве средства совершения деяния. Такие составы имеются практически в каждом разделе Уголовного кодекса Туркменистана и обычно в уголовно-правовой доктрине их принято обозначать как общеуголовные составы преступлений. Объектами таких преступлений являются различные блага, охраняемые законом, например, экономическая деятельность, мир и государство, общественная безопасность и т.д[1].

Однако не каждое преступление с практической точки зрения может быть совершено посредством использования информационных технологий, хотя тенденция прогрессивного развития цифровых технологий в будущем может внести коррективы в это утверждение, ввиду того, что многие преступления предполагают под совершением противоправного деяния физическое воздействие, например, преступление против личности (убийство). Очевидно, что, используя компьютер или телефон, невозможно убить человека, либо нанести ему увечья, но, например, довести его до самоубийства либо заставить совершить определенные действия или повлиять на работу банка, изменить данные банковского счета весьма возможно.

Исходя из изложенного следует сказать, что законодатель Туркменистана отошел от традиционной нам системной организации вышеуказанных деликтов, хотя сохранил отдельные издержки в виде составов преступлений, и сосредоточился на разработке уголовно-правовых механизмов регулирования и пресечения противоправных деяний в сфере компьютерной информации. В этом смысле прогрессивная система развития уголовного законодательства Туркменистана вызывает интерес дальнейшего наблюдения.

---

[1] Уголовный Кодекс Туркменистана от 12 июня 1997 № 222-I. [Электронный ресурс]. URL: online.zakon.kz/Document/? Doc_id=3129586 (дата обращения: 21.07.2024).

В заключение важно отметить, что развитие и внедрение информатизации в государственную, экономическую и социальную сферы жизни Туркменистана (об этом свидетельствует государственная политика Туркменистана, направленная на цифровизацию)[1] предопределяет совершенствование уголовного законодательства Туркменистана в направлении противодействия преступлениям в сфере цифровых имущественных отношений. Уголовно-правовое противодействие преступлениям в сфере цифровых имущественных отношений становится одним из ключевых аспектов обеспечения правопорядка и защиты прав граждан, в связи с этим возникает необходимость в разработке и внедрении новых уголовно-правовых норм. Предлагается ввести в Уголовный кодекс Туркменистана ст. 249[1] «Хищение в сфере цифровых средств». Это дополнение должно предусматривать уголовную ответственность за преступления, связанные с получением незаконной личной выгоды в форме различных видов имущества, включая электронные денежные средства (криптовалюта), другие цифровые имущественные ценности (электронные файлы, цифровые рукописи, ценные бумаги и др.). Внедрение первой уголовно-правовой нормы в сфере цифровых имущественных отношений в Уголовный кодекс Туркменистана позволит защитить имущественные блага граждан страны.

1.3. Состояние и динамика преступлений в сфере компьютерной информации и иных преступлений, совершаемых с использованием информационно – телекоммуникационных сетей (технологий), в Российской Федерации и Туркменистане

[1] Цифровизация – ключевой фактор экономического развития. [Электронный ресурс]. URL.: https://www.turkmenistan.gov.tm/ru/post/86889/cifrovizaciya-klyuchevoj-faktor-ekonomicheskogo-razvitiya.

Основным средством повышения уровня производительности является развитие цифровых инструментов. Главными мерами развития экономических отраслей является широкое внедрение информационных технологических средств в данные отрасли. Информационные и телекоммуникационные системы, технологии выделяются как приоритетные компоненты для широкого развития технологического общества и передового технологического развития государствообразующих институтов.

За последние годы в Российской Федерации и Туркменистане создана широкая нормативная правовая база, направленная на развитие цифровой экономики с учетом современных трендов в сфере научно-технологического развития «умных городов». Также помимо нормативного правового регулирования одним их основных толчков внедрения цифровых технологий стала пандемия, которая подразумевала переход на удаленную работу, а также обеспечение электронного доступа к таким сферам человеческой жизнедеятельности, как здравоохранение, образование, экономика.

Активное развитие получил и онлайн-банкинг, способствующий активному финансовому взаимодействию различных сфер экономического кластера. На основании данного развития в Туркменистане и Российской Федерации увеличилось количество пользователей интернет-банкинга, а также число банковских карт. В Туркменистане такими пользователями являются более 5 миллионов человек, в Российской Федерации более 390 млн пользователей, в том числе нерезидентов.

В связи с этим в настоящее время мы наблюдаем значительный рост числа связанных с онлайн-банкингом преступлений, которые происходят в пределах Российской Федерации и Туркменистана. Это явление становится все более тревожным и требует особого внимания как со стороны правоохранительных органов, так и со стороны самих пользователей банковских интернет-сервисов.

С развитием технологий и переходом большого количества финансовых операций в онлайн-пространство мошенники находят все новые и новые способы незаконного завладения чужими денежными средствами. В связи с этим в Российской Федерации и Туркменистане зафиксировано увеличение количества случаев, когда злоумышленники, используя различные виды хакерских атак, фишинг и другие методы обмана, совершают противоправные действия, направленные на хищение средств с банковских счетов граждан.

Такие действия наносят серьезный ущерб не только отдельным клиентам банков, но и подрывают доверие к системе онлайн-банкинга в целом, что может привести к дестабилизации финансовой системы страны. Поэтому проблема киберпреступности в сфере онлайн-банкинга в Российской Федерации и Туркменистане требует незамедлительного реагирования и разработки эффективных мер по предотвращению и борьбе с данным видом преступлений.

Глобальный всплеск киберпреступности во многих странах мира, в том числе в Российской Федерации и Туркменистане, связан активным развитием глобальной сети «Интернет», сопряженным в том числе с развитием экономических преобразований основных сфер общественной жизни. По проведенным опросам правоохранительных органов в части совершения компьютерных преступлений отмечается высокий уровень роста в связи с тем, что у заинтересованных физических лиц, а также различных организованных групп появилась возможность для совершения преступлений с целью получения выгоды финансового и имущественного характера.

Основная масса таких преступлений – по последним данным это порядка 80% - совершаются путем организации комплексной деятельности с формированием черного рынка киберуслуг, связанных с масштабным созданием алгоритмов вредоносных программ с целью обхода программных барьеров, заражением компьютерной системы, созданием различных сетей с искусственным интеллектом, выполняющим определённые задачи, в том

числе сбор персональных данных пользователей, данных финансового характера, предложение фейковых услуг в качестве модератора.

Вместе с тем среди заинтересованного контингента людей – обычно это молодые люди, обладающие знаниями в сфере компьютерной информации, - создаются сообщества по интересам, направленные на совершения преступлений, а именно финансового мошенничества. Развитие цифровых экономических ниш, сферы услуг, внедрение данных в цифровую сеть создают возможности таким лицам использовать цифровые технологии в корыстных целях.

Евразийский континент активно развивается в направлении цифровой трансформации экономической, промышленной инфраструктуры с внедрением сети «Интернет» в общественную жизнь. Одним из самых актуальных и быстрых способов получения информации как раз и являются информационно-телекоммуникационные сети, по котором передаются многие виды информации, в том числе новостная, государственная, частная, личная. В связи с информатизацией общественных институтов у людей возрастает потребность в цифровых средствам связи, в том числе смартфоны, компьютеры и т.д. Согласно статистическим данным число пользователей цифровыми средствами связи, интернет сетями в СНГ составляет примерно около 71,3 % от общего числа населения[1].

Сосредоточение огромного массива в руках такого большого числа людей информации, обмен данной информацией приводит к низкому уровню защищенности информации, так как огромная информационная сеть замыкается в рамках серверов, компьютеров, которые и являются местом проникновения злоумышленников с целью перехвата, завладения и уничтожения информации. Любая цифровая информация имеет определённые точки выхода и входа (накопители), на практике такими

[1] [Электронный ресурс]. URL: https://news.un.org/ru/story/2018/12/1344531 (дата обращения 22.05.2024).

точками являются сервера, компьютеры, телефоны, и нужно понимать, что любая цифровая система имеет уязвимые места в цепочке передачи информации.

Информационное пространство евразийского региона весьма разнообразно, так как во многих государствах имеются ограничения в использовании цифровой информации, и зачастую это связано с низким уровнем цифровизации, отсутствием инвестиционной составляющей в развитии информационной инфраструктуры. Организация Объединённых Наций по итогам 2023-2024 годов зафиксировала рост пользователей сети «Интернет»: таковых на сегодняшний день около 5,5 миллиардов человек[1]. Что касается Российской Федерации и Туркменистана, то в первой пользователями являются 130 миллионов человек при общем населении 146 миллионов[2], тогда как во второй пользователями являются 3 149 178 человек с общим населением 7 364 000 человек[3]. Примерно 89,04%[4] населения России активно используют цифровое пространство в повседневной жизни, тогда как в Туркменистане 42,7%[5] населения на данный момент являются активными пользователями цифровых технологий. При этом за примерно за год динамика группы пользователей растет на 3-4 %, и если прогнозировать прогрессию, то примерно через 5 лет число таких пользователей будет в разы больше[6].

В этом контексте, если сравнивать Туркменистан и Российскую Федерацию, становится очевидным, что в России число людей, погруженных в виртуальное пространство, значительно превышает туркменские показатели. Это различие можно объяснить несколькими ключевыми факторами.

---

[1] [Электронный ресурс]. URL: https://news.un.org/ru/story/2024/11/1458816 (дата обращения 24.04.2024).
[2] [Электронный ресурс].URL:https://www.rbc.ru/technology_and_media/11/12/2024/6759b4709a79472b45d8949e (дата обращения 24.04.2024).
[3] [Электронный ресурс]. URL: https://turkmenistan.gov.tm/ru/post/77372/vse-naselennye-punkty-turkmenistana-obespecheny-vysokoskorostnym-internetom (дата обращения 24.04.2024)
[4] 130 млн.:146 млн.*100=89,04%.
[5] 3149178:7364000*100=42,76%.
[6] Global Cybersecurity Index 2020 // ITU Publications. [Электронный ресурс]. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STRGCI.01-2021-PDF-E.pdf. (дата обращения 24.04.2024).

Прежде всего, Россия обладает более мощной и разветвленной информационной инфраструктурой. В стране активно развиваются сети связи, повышается доступность и скорость интернет-соединения, что делает веб более доступным для широких слоев населения. К тому же, Российская Федерация имеет значительно большее количество жителей, что автоматически увеличивает потенциальную аудиторию пользователей интернета.

Таким образом, сравнительно меньшее число интернет-пользователей в Туркменистане можно объяснить менее развитой информационной инфраструктурой и меньшим населением страны по сравнению с Российской Федерацией. Эти факторы играют решающую роль в формировании цифрового ландшафта обеих стран. Согласно докладам глобального индекса кибербезопасности (GCI) особенно уязвимыми к киберугрозам оказался Туркменистан, занявший 138 место в рейтинге[1]. Также Туркменистан входит в пятерку стран Центральной Азии по уровню киберактивности злоумышленников в финансовой сфере.

Кроме того, зафиксировано, что Туркменистане происходят активные попытки внедрения различных программ с целью латентной генерации электронной валюты в обход контрольной информационной инфраструктуры. По последним данным Туркменистан входит в первую десятку стран с большим показателей таких преступных деяний.

В наше время цифровая экономика развивается бурными темпами, и виртуальные деньги стали неотъемлемой частью этого процесса. Однако вместе с легальными методами майнинга и обращения криптовалют, возникают и незаконные пути их создания и использования. Неправомерное производство цифровых денег подрывает основы экономической

---

[1] Global Cybersecurity Index 2020 // ITU Publications. [Электронный ресурс]. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STRGCI.01-2021-PDF-E.pdf. (дата обращения 24.04.2024).

стабильности и безопасности, ведь оно часто связано с мошенничеством, отмыванием денег и другими видами преступной деятельности.

Криптовалюты, такие как Биткоин и Эфириум, привлекают внимание не только инвесторов, но и злоумышленников, желающих нажиться недобросовестным путем. Незаконный майнинг может осуществляться с использованием вирусного ПО, которое заражает компьютеры ничего не подозревающих пользователей и использует их вычислительные мощности для добычи криптовалют без ведома владельцев. Также распространено создание фальшивых платформ для инвестирования в цифровые валюты, где вкладываются средства, но возврата не происходит.

Помимо прямого ущерба для пользователей, неправомерное производство цифровых денег несет в себе и широкомасштабные риски. Оно подрывает доверие к криптовалютному рынку, создает предпосылки для нестабильности и спекуляций, а также может служить инструментом для финансирования терроризма и других противозаконных активностей.

Следовательно, противодействие нелегальному производству и обороту цифровой валюты является важнейшей задачей для государственных органов Туркменистана и Российской Федерации. В данный момент времени государственно-правовым инструментом этого противодействия для обоих государств является разработка и внедрение эффективных механизмов контроля и регулирования, усиление правоприменительной практики и повышение осведомленности общества о рисках, связанных с криптовалютами.

Вместе тем согласно аналитическим отчетам Лаборатории Касперского Туркменистан занимает первое место среди стран азиатского региона, пользователи интернет-ресурсов которых наибольшее число раз подвергались различному цифровому заражению с использованием вирусных программ, около 58% пользователей столкнулись с локальным заражением, а именно с процессом заражения компьютерной системы вредоносным программным

обеспечением (Malware) через локальные источники, такие как инфицированные USB-накопители, зараженные файлы или программы, вредоносные скрипты и другие локальные угрозы. Локальное заражение вирусными программами — это процесс, при котором вредоносные программы, такие как вирусы, трояны или шпионское ПО, проникают в систему через носители информации, подключаемые к компьютеру, например, через USB-накопители, CD/DVD-диски или внешние жесткие диски. Это контрастирует с удаленным заражением, когда вирусы распространяются через интернет или локальные сети. Локальное заражение часто происходит из-за использования нелицензионного программного обеспечения или файлов, скачанных с ненадежных источников[1].

В свою очередь, Россия входит в число 10 стран по доле пользователей, подвергшихся локальным атакам, около 3,83 % пользователей атакуется на локальном уровне ежедневно. Также Россия входит в топ 10 стран по числу кибератак за год, по последним данным около 1,8 млрд кибератак совершаются ежегодно[2].

В число таких входят преступления с применением Telnet. Telnet — это простой протокол сетевого доступа, который может быть использован для удаленного управления компьютером или устройствами, но при этом он не обеспечивает аутентификацию или шифрование, что делает его уязвимым для атак.

Как мы можем заметить, в Российской Федерации и Туркменистане наблюдается рост киберпреступности, что становится серьезной проблемой для стран. Анализируя данные о преступлениях в сфере информационных технологий, можно заметить увеличение количества инцидентов, связанных с несанкционированным доступом к данным, мошенничеством в интернете и

---

[1] См.: [Электронный ресурс]. URL.: https://statistics.securelist.com/ru/country/turkmenistan/intrusion-detection-scan/month (дата обращения: 24.05.2025).

[2] См.: [Электронный ресурс]. URL.: https://www.gazeta.ru/tech/news/2025/01/16/24840404.shtml (дата обращения: 24.05.2025).

другими видами кибератак. Это вызывает обеспокоенность у правительства и требует принятия мер для усиления кибербезопасности. Укрепление законодательства и повышение осведомленности граждан о рисках в сети являются ключевыми аспектами в борьбе с киберпреступностью.

Проблематика компьютерных преступлений упирается в возможность дистанционного совершения деяния. Практически преступление компьютерного характера может быть совершено из любой точки мира при условии обеспечения этой точки сетью «Интернет». Данный аспект является проблематикой для правоохранительных органов в части привлечения лица к ответственности. Данные проблемные аспекты практически ежегодно затрагиваются главами государств на различных политических площадках, на которых активно обсуждается роль информационных технологий в современном мире. Обращаясь к коллегии Министерства внутренних дел Российской Федерации в 2021 г., Президент Российской Федерации В. Путин заявил: «…технологии быстро развиваются, мы за ними, к сожалению, не успеваем. Все мы хорошо понимаем при этом, что за развитием электронной торговли, за предоставлением в глобальной сети разного рода услуг, включая финансовые услуги, – за этим, конечно, будущее. Технологии здесь обновляются и меняются стремительно, но и поле для преступлений, для разного рода аферистов, к сожалению, тоже увеличивается»[1]. Президент Туркменистана в ходе правительственного совещания подписал постановление «О намеченных мерах усиления работ по обеспечению кибербезопасности в Туркменистане», а также отметил, что одним из требований времени выступает укрепление кибербезопасности страны [2].

Целью злоумышленников является не только финансовые блага, но и различные личные данные человека, в том числе банковские счета,

---

[1] См.: [Электронный ресурс]. URL: https:// kremlin.ru/events/president/news/65090 (дата обращения: 22.01.2023).
[2] См.: [Электронный ресурс]. URL:https://bigasia.ru/turkmenistan-usilit-mery-po-obespecheniyu-kiberbezopasnosti/ (дата обращения: 22.01.2023)

паспортные данные, номера телефонов и т.д. А если говорить в рамках государства, то под угрозу преступления могут попасть не только правительственные организации, органы власти, но и предприятия, специализирующие в сфере атомной энергетики, ракетно-космической техники: взлом данных, их повреждение, уничтожение, воздействие на данные в таком случае может привести к необратимым последствиям. Поступательное развитие информационных технологий и возможность их использования в незаконных целях привело к появлению такого термина, как «информационное оружие», вполне справедливо отражающего в лексическом смысле угрозу определенным объектам воздействия данного оружия. По мнению многих исследователей, информационное оружие по масштабам ущерба имеет все возможности стать опаснее, чем оружие массового поражения, такое, как ядерное.

Например, можно привести ряд громких преступлений в данной сфере. В январе 2021 года DDoS-атаке подвергся ИТ-гигант «Яндекс». По сообщениям пресс-службы корпорации, эта атака стала самой масштабной за всю историю существования корпорации. На сегодняшней день лица, совершившие деяние, не найдены[1]. В ноябре 2024 года Министерство цифрового развития Российской Федерации сообщило об отражении огромного количества кибератак на государственный портал «Госуслуги» (более 700 гигабит в секунду)[2]. Также в июле 2015 года хакерами был атакован сервер Международного агентства по атомной энергетике, хакерами было украдено и в дальнейшем размещено в общий доступ в сети Интернет персональные данные двух тысяч сотрудников организации[3]. И это лишь громкие преступления. На самом деле каждый день происходят тысячи DDoS атак на частные организации, банки, органы государственной власти,

---

[1] См.: [Электронный ресурс]. URL: https://stormwall.pro/resources/blog/ddos-ataka-na-yandex (дата обращения: 25.04.2025).
[2] См.: [Электронный ресурс]. URL: https://tass.ru/obschestvo/19956881 (дата обращения: 25.04.2025).
[3] См.: [Электронный ресурс]. URL: https://peretok.ru/articles/trading/14057/ (дата обращения: 25.04.2025).

международные организации. А с развитием цифровых технологий количество данных преступлений увеличивается, соответственно и увеличивается число пострадавших лиц. В большинстве случаев правоохранительные органы отказывают в возбуждении уголовного дела в связи с отсутствием состава преступления (невозможностью установить лицо, совершившее данное деяние).

Также основной массой жертв преступников по статистическим данным становятся лица с низким уровнем грамотности в сфере цифровых и информационных технологий. Мошенники производят рассылку различных ссылок, документов, направляют сообщения в социальных сетях, мессенджерах с мотивировочным сообщение о том, что это важно для пользователя и, перейдя по данной ссылке, он сможет приумножить свой капитал, а в результате происходит внедрение вируса на цифровое устройство и утеря персональных данных, электронных денежных средств и т.д.

Та же самая история, но с более серьезным ущербом происходит в различных учреждениях, государственной, частной собственности, когда злоумышленники отправляют документы, электронные ссылки на корпоративную почту работников или учреждения в целом, приводят к тому, что работник, проходя по ссылке или открывая документ, запускает в систему организации вирусную программу, которая уничтожает ее изнутри и поглощает огромное количество информации. В конечном итоге это приводит к простою организации и огромному ущербу.

Различного рода цифровые техники позволяют злоумышленникам действовать инкогнито, не оставляя своих следов (данных), а также позволяют совершать данные деяния с территории других государств, а в некоторых случаях действовать группой лиц, участники которой находятся на территории других стран. Зачастую злоумышленники подбирают страну (место дислокации) с учётом того, что у данной страны нет международного договора

об экстрадиции со страной, против которой планируется совершение преступления.

Динамика роста таких преступлений ежегодно формируется и публикуется правоохранительными органами, в частности МВД, и она показывает увеличение числа таких преступлений. Статистика за последние 4 года выглядит следующим образом[1].

Рисунок 1

Как мы видим, рост таких преступлений в числовом соотношении достаточно велик, при этом на увеличение таких преступлений влияют различные политические, экономические аспекты, развитие цифровых денег. Процентное соотношение за 4 года показывает умеренный рост между 2021 и 2022 гг., который составил 0,8 %, далее в 2023 г. прирост преступлений

[1] Состояние преступности в Российской Федерации за январь - декабрь 2020 года. [Электронный ресурс]. URL: https://xn--b1aew.xn--p1ai/reports/item/22678184/ (дата обращения: 26.03.2025).
Состояние преступности в Российской Федерации за январь - декабрь 2021 года. [Электронный ресурс]. URL: https://xn--b1aew.xn--p1ai/reports/item/28021552/ (дата обращения: 26.03.2025).
Состояние преступности в Российской Федерации за январь - декабрь 2022 года. [Электронный ресурс]. URL: https://xn--b1aew.xn--p1ai/reports/item/35396677/ (дата обращения: 26.03.2025)
Состояние преступности в Российской Федерации за январь - декабрь 2023 года. [Электронный ресурс]. URL: https://xn--b1aew.xn--p1ai/reports/item/47055751/ (дата обращения: 26.03.2025).
Состояние преступности в Российской Федерации за январь - декабрь 2024 года. [Электронный ресурс]. URL: https://xn--b1aew.xn--p1ai/reports/item/60248328/ (дата обращения: 26.03.2025).

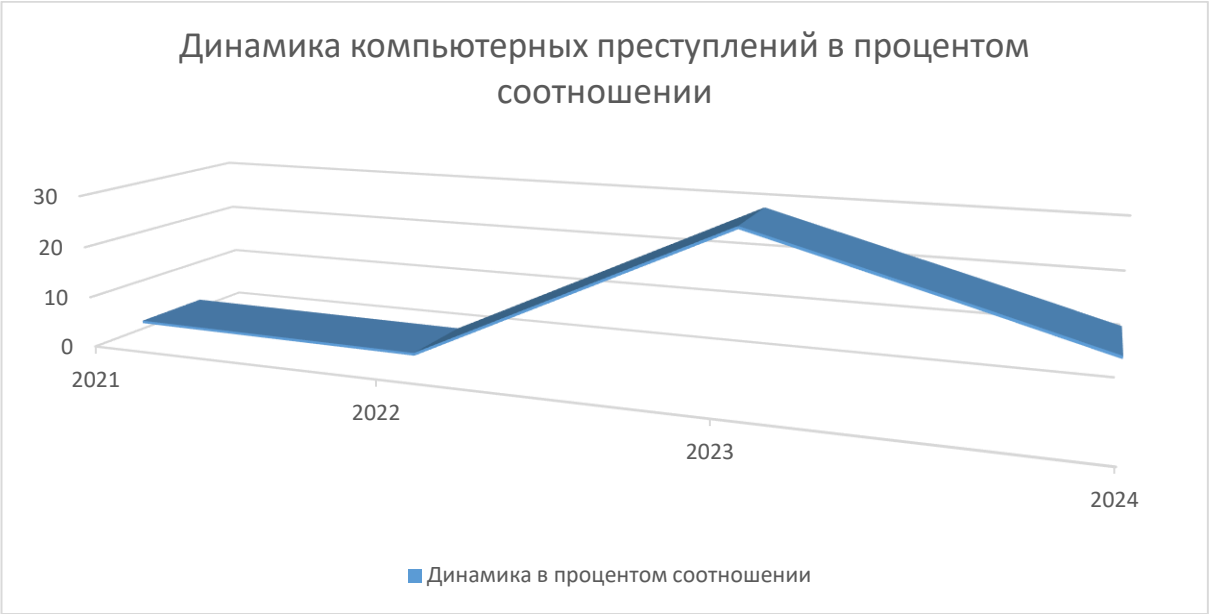
достигает максимума в 30%. Снова виной негативной динамики является кибермошеничество[1].

В связи с этим основной удар приходится на банковский сектор, интернет-банкинг, а также портал «Госуслуги». Основная цель злоумышленников - завладеть данными граждан России, а также получить доступ к банковским операциям. На этом фоне увеличивается телефонный шантаж, приводящий к утере доступа граждан к своим электронным банковским программам с последующим снятием со счетов денежных средств. Данную категорию также называют дистанционным мошенничеством, когда на территории других стран открываются колл-центры, осуществляющие мошеннические действия. В 2024 г. происходит небольшой спад отрицательной динамики таких преступлений (таблица № 2).

Рисунок 2[2]

[1] Состояние преступности в Российской Федерации за январь - декабрь 2021 года. [Электронный ресурс]. URL: https://xn--b1aew.xn--p1ai/reports/item/28021552/ (дата обращения: 26.03.2025).

[2] Состояние преступности в Российской Федерации за январь - декабрь 2020 года. [Электронный ресурс]. URL: https://xn--b1aew.xn--p1ai/reports/item/22678184/ (дата обращения: 26.03.2025).
Состояние преступности в Российской Федерации за январь - декабрь 2021 года. [Электронный ресурс]. URL: https://xn--b1aew.xn--p1ai/reports/item/28021552/ (дата обращения: 26.03.2025).
Состояние преступности в Российской Федерации за январь - декабрь 2022 года. [Электронный ресурс]. URL: https://xn--b1aew.xn--p1ai/reports/item/35396677/ (дата обращения: 26.03.2025)
Состояние преступности в Российской Федерации за январь - декабрь 2023 года. [Электронный ресурс]. URL: https://xn--b1aew.xn--p1ai/reports/item/47055751/ (дата обращения: 26.03.2025).
Состояние преступности в Российской Федерации за январь - декабрь 2024 года. [Электронный ресурс]. URL: https://xn--b1aew.xn--p1ai/reports/item/60248328/ (дата обращения: 26.03.2025).



Активно используются для совершения дистанционного мошенничества мессенджеры, такие как «Telegram» и «WhatsApp», злоумышленники создают недействительные, «фейковые» аккаунты и начинают писать или звонить другим людям, представляясь сотрудниками спецслужб. Яркий пример можно привести из личной практики работы в Самарском университете им. Королева, когда злоумышленник создал фейковый аккаунт руководителя учреждения, установив при этом в качестве аватара его фотографию с сайта, и написал от имени руководителя работникам организации о том, что им срочно нужно связаться с сотрудником специальных служб, так как адресат сообщения является подозреваемым по уголовному делу. Если бы сотрудник вышел на контакт с мошенником, это привело бы к переводу денежных средств на счет злоумышленников, либо к предоставлению им данных, позволяющих получить доступ к банковским картам и счетам в банках.

Еще один яркий пример дистанционного мошенничества произошел в 2025 г. в городе Самара. Пенсионерке позвонили по телефону и представились сотрудниками специальных служб, ей сообщили, что преступники получили доступ к её счетам в банке и осуществляют перевод денег за границу. Женщина сняла с со своего счета наличными 421 миллион рублей и передала курьеру, якобы для сохранения денежных средств. Впоследствии она пришла

в банк повторно с целью обналичить оставшуюся сумму, однако сотрудники банка поняли о предположительном факте мошенничества, о чем сообщили в правоохранительные органы[1].

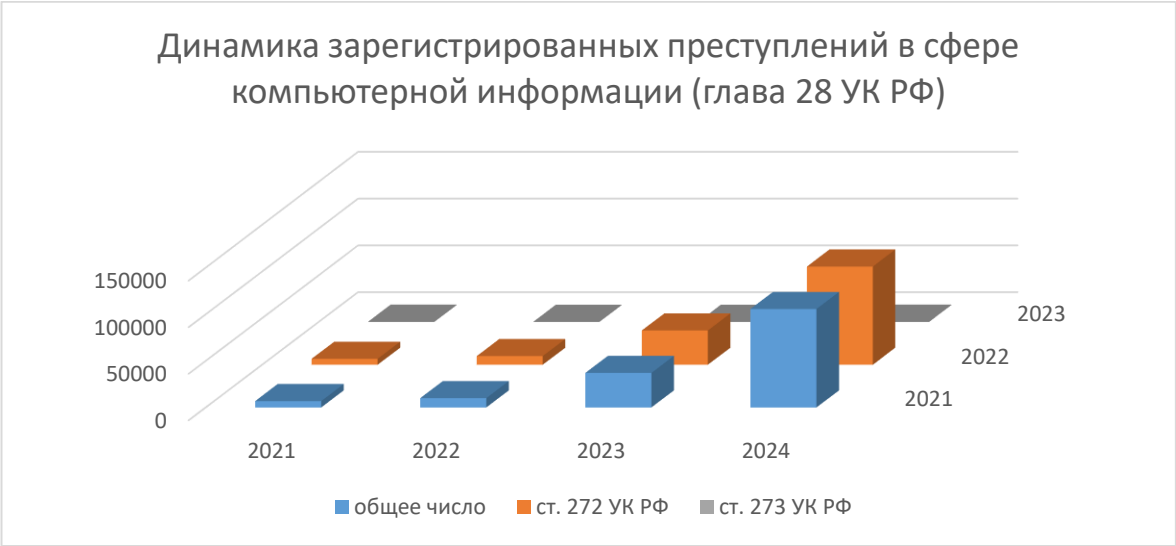
Если из всего массива компьютерных преступлений выделять преступления в сфере компьютерной информации, то можно сказать, что число таких преступлений небольшое в соотношении со всеми видами преступлений, совершаемых в информационном пространстве. Согласно официальным данным таких преступлений за 2021 г. выявлено около 6900, за 2022 г. – 10 027, за 2023 г. - 37 101, за 2024 г. – 52 000 (таблица 3). Количество таких преступлений увеличилось в примерно в 6 раз за 4 года. Кроме того, если анализировать статистику по каждому составу преступлений в сфере компьютерной информации, то следует заключить, что 98% преступлений совершается по ст. 272 УК РФ, остальные 2% - это преступления, предусмотренные ст. 273 УК РФ[2].

Рисунок 3

---

[1] См.: Задержаны мошенники, похитившие 421 миллион у пенсионерки из Самары. [Электронный ресурс]. URL: https://rg.ru/2025/02/11/zaderzhany-moshenniki-pohitivshie-421-million-u-pensionerki-iz-samary.html (дата обращения: 12.02.2025).

[2] Состояние преступности в Российской Федерации за январь - декабрь 2020 года. [Электронный ресурс]. URL: https://xn--b1aew.xn--p1ai/reports/item/22678184/ (дата обращения: 26.03.2025).
Состояние преступности в Российской Федерации за январь - декабрь 2021 года. [Электронный ресурс]. URL: https://xn--b1aew.xn--p1ai/reports/item/28021552/ (дата обращения: 26.03.2025).
Состояние преступности в Российской Федерации за январь - декабрь 2022 года. [Электронный ресурс]. URL: https://xn--b1aew.xn--p1ai/reports/item/35396677/ (дата обращения: 26.03.2025)
Состояние преступности в Российской Федерации за январь - декабрь 2023 года. [Электронный ресурс]. URL: https://xn--b1aew.xn--p1ai/reports/item/47055751/ (дата обращения: 26.03.2025).
Состояние преступности в Российской Федерации за январь - декабрь 2024 года. [Электронный ресурс]. URL: https://xn--b1aew.xn--p1ai/reports/item/60248328/ (дата обращения: 26.03.2025).



Использование метода соотношения динамики киберпреступности в России и Туркменистане позволяет сделать вывод, что по уровню индекса цифровой защищённости на территории СНГ Россия занимает лидирующие позиции, а Туркменистан в этом плане занимает последние позиции из всех стран СНГ[1]. При этом уровень компьютерных атак в России фиксируется за год выше, чем в Туркменистане[2]. Такой разрыв в первую очередь связан с нескольким разными факторами, в том числе с количеством населения, уровнем развития информационной системы, потенциалом инфраструктуры, обеспечивающей защиту информационного пространства страны. Ниже представлена статистика таких деяний.

По открытым статистическим данным и анализу динамики цифровых преступлений различной формации в Туркменистане ежемесячно от общего числа преступлений фиксируется 48 % компьютерных атак с помощью программ-вымогателей, 25% веб-угроз, 27 % локальных атак (банки и государственные организации)[3].

---

[1] [Электронный ресурс]. URL: https://ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-v-stranah-sng-2023-2024/#id2 (дата обращения 21.05.2025).

[2] Рейтинг стран по уровню кибербезопасности. [Электронный ресурс]. URL: https://statistics.securelist.com/ru/ransomware/month (дата обращения 23.01.2024).

[3] Статистика киберугроз в Туркменистане. [Электронный ресурс]. URL: https://statistics.securelist.com/ru/country/turkmenistan/ransomware/day (дата обращения: 26.03.2025).

Исходя из данных «Лаборатории Касперского», основные угрозы, которые фиксируются лабораторией, направлены на государственные органы, а также банковскую сферу. Основными инструментами проникновения по Туркменистану стали программы-вымогатели, спам, вредоносная почта, сетевые атаки, эксплойты[1]. 51 % подобных преступлений за каждый месяц совершается с использованием вредоносных программ разной формации таких как троян, распространение спама[2].

Вместе с тем конгломерат всех преступлений в сфере компьютерной информации и иных видов преступлений, совершаемых с использованием информационных технологий в Туркменистане, можно разделить на 2 основные группы.

1. Преступления, целью которых являются банковский сектор экономики. С помощью использования вредоносного программного обеспечения оказывается негативное воздействие на работу сервисов и информационной системы банка, государственных банков, в частности «Дайханбанка», «Халкбанка», банка «Туркменистан», а также коммерческих банков, в частности банков «Сенагат» и «Гарагум». Суммарный ущерб может составлять несколько десятков миллионов долларов.

2. Преступления, целью которых является государственно-политический блок. Сюда входят атаки на критическую инфраструктуру Туркменистана, на национальную информационную систему, сайты и сервера государственных органов, включая министерства, правительственные организации. Удар по экономической, информационной, общественной безопасности страны является огромным. Можно сказать, что Российская Федерации и Туркменистан, страны – стратегические партнеры, которые подвержены своеобразному «цифровому испытанию», когда в государстве вынуждены

---

[1] См. Статистика киберугроз в Туркменистане. [Электронный ресурс]. URL: https://statistics.securelist.com/ru/ransomware/month (дата обращения 23.01.2024).

[2] См. Там же.

развивать систему информационной защиты. Столь стремительное развитие информационных технологий подвергает ежедневным испытаниям как обычных людей, так и огромные государственные корпорации. В этом смысле вспоминаются слова П. Коэльо из романа «Алхимик»: «Золото является металлом, эволюция которого зашла дальше остальных металлов. Такая тенденция повелась в мире, так как люди иным образом истолковали слова мудрецов. И вместо того, чтобы стать символом развития, сделалось символом раздора»[1]. Эти слова объясняют всю сущность существования информационных технологий. Да, сотни фантастов 20 века писали о прекрасном цифровом будущем, о мире, который будет роботизирован. Вокруг концепции трансгуманизма сформировалось целое философское направление. Действительно, мир стал таким и дальше эволюционирует в части информационного наполнения общественной жизни. Однако технологии, которые, как планировалось, должны были улучшить жизнь человека и общества, стали угрозой для них, а также для государства и мира в целом.

[1] См. Коэльо Пауло «Алхимик»: [роман] / Пауло Коэльо; [пер. с португальского А. Богдановского]. Москва: Издательство АСТ, 2025. С. 187.

Глава 2. Соотношение основных составов преступлений в сфере компьютерной информации по современному уголовному законодательству России и Туркменистана

2.1. Особенности объективных признаков преступлений в сфере компьютерной информации по современному уголовному законодательству России и Туркменистана[1]

Вопросы объективных признаков преступлений в сфере компьютерной информации являются обширным полем для дискуссии, вопросы определения объективной стороны, объекта, средств совершения, способов совершения, предмета в уголовно-правовой науке не имеют единых подходов.

Объект[2].

Преступления в сфере компьютерной информации и иные преступления, совершаемые с использованием информационно-телекоммуникационных сетей (технологий), являются обширной группой преступлений многообъектного характера[3]. Объектами таких деяний могут быть множество благ, охраняемых уголовным законодательством. Такая позиция вписывается в структурную особенность уголовного законодательства Российской Федерации и Туркменистана[4].

---

[1] См. Корпеев, А.Г. Об объекте преступлений, совершаемых с использованием информационно-телекоммуникационных сетей, по уголовному законодательству России и Туркменистана // Юридический аналитический журнал. 2022. 17 (1). С. 29–33; Корпеев А.Г. О предмете преступлений, совершаемых с использованием информационно-телекоммуникационных сетей, по уголовному законодательству Российской Федерации и Туркменистана // Юридический аналитический журнал. 2023. 18 (1). С. 20-24; См.: Корпеев, А.Г. Средства совершения преступлений в сфере компьютерной информации по уголовному законодательству Российской Федерации и Туркменистана // Юридический вестник Самарского университета Juridical Journal of Samara University. 2025. Т. 11, № 2. С.96-102.

[2] См.: Корпеев, А.Г. Об объекте преступлений, совершаемых с использованием информационно-телекоммуникационных сетей, по уголовному законодательству России и Туркменистана // Юридический аналитический журнал. 2022. 17 (1). С. 29–33

[3] Данную позицию поддержали 95,8 % опрошенных респондентов.

[4] См. Корпеев, А.Г. Об объекте преступлений, совершаемых с использованием информационно-телекоммуникационных сетей, по уголовному законодательству России и Туркменистана // Юридический аналитический журнал. 2022. 17 (1). С. 29–33

На основании структурной универсальности УК РФ и УК Туркменистана (глава 28 УК РФ, глава 33 УК Туркменистана, а также совокупность иных преступлений, совершаемых с использованием информационно-телекоммуникационных технологий), содержание родового, видового и непосредственного (основного и дополнительных) объектов таких преступлений логично было бы определять следующим образом[1].

Родовым объектом преступлений в сфере компьютерной информации является группа общественных отношений, образующих родовую линию исходя из правовой природы таких отношений: общественная безопасности, отношения в сфере безопасности компьютерной информации (на примере раздела 13 УК Туркменистана»)[2].

При этом родовыми объектами преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (технологий), по уголовному законодательству Российской Федерации и Туркменистана является многообразие благ, обозначенных уголовным законодательством как приоритетные общественные отношения, влияние на которые возможно с применением различных информационных технологий: безопасность мира и человечества, отношения в сфере экономики, интересы личности, а также безопасности государственной власти и т.д[3].

Видовой объект таких отношений формируется исходя из родственных родовому объекту общественных отношений, обозначенных как составной элемент родового объекта: отношения в сфере безопасности компьютерной информации, безопасность информатики и связи (глава 33 УК Туркменистана), интересы семьи и несовершеннолетних, жизнь и здоровье, отношения в сфере собственности, мир и безопасность человечества, экономическую деятельность.

---

[1] См.: Там.же.
[2] См.: Там же.
[3] См.: Там же.

Непосредственный объект образуют различные категорированные блага: конкретизированные конституционные права и свободы человека, жизнь человека, безопасность человечества, информационную безопасность, безопасность государства, а также материальные блага в виде собственности физических лиц, отношения в сфере обращения денег, ценных бумаг, цифровой валюты[1].

Обязательный дополнительный объект: особый сегмент общественной безопасности – информационная безопасность. В контексте рассматриваемой проблематики информационная безопасность – это такое центральное правоохраняемое благо, которое всегда является либо основной, либо вспомогательной целью названных преступлений[2].

Вместе с тем, определяя общественную безопасность обязательным дополнительным объектом, важно отметить, что речь идет о важном виде общественной безопасности – безопасность информационного пространства, в том числе и информационно-телекоммуникационных сетей[3].

По своей сути многообразие различных благ, защищаемых уголовным законодательством, всегда являются совокупной частью безопасности. Исходя из этого, если общественная опасность выступает свойством любого преступления, то из этого можно сделать вывод, что преступления как общественно опасное явление являются нарушением целостности системы безопасности[4]. Таким образом, следует полагать, что компьютерную

---

[1] См. Корпеев, А.Г. Об объекте преступлений, совершаемых с использованием информационно-телекоммуникационных сетей, по уголовному законодательству России и Туркменистана // Юридический аналитический журнал. 2022. 17 (1). С. 29–33

[2] См. Корпеев, А.Г. Об объекте преступлений, совершаемых с использованием информационно-телекоммуникационных сетей, по уголовному законодательству России и Туркменистана // Юридический аналитический журнал. 2022. 17 (1). С. 29–33

[3] См.: Там же.

[4] См.: Юрченко, И.А. Преступления против безопасности информации, преступления против информационной безопасности, преступления информационной направленности: определение понятий // УГОЛОВНОЕ ПРАВО: СТРАТЕГИЯ РАЗВИТИЯ В XXI ВЕКЕ материалы XIV Международной научно-практической конференции. Министерство образования и науки Российской Федерации; Московский государственный юридический университет имени О. Е. Кутафина (МГЮА). Москва, 2017. С. 477-480.

безопасность, а равно информационную безопасность стоит рассматривать в роли дополнительного объекта такого рода преступлений.

Предмет[1].

Рассматривая предметную составляющую преступлений, следует обратить внимание на природу происхождения таких предметов: основываясь на уголовной доктрине, предметом преступлений следует считать материальные объекты мира, разной типологии, являющиеся ценными с точки зрения уголовного законодательства[2].

Вопрос определения предмета является частью философской материальной концепции. Материальная концепция предмета выражается в его физическом бытии, воплощении материи в реальной визуально-осязаемой проекции. При этом вещь представляется как объективный, устойчивый компонент, реализованный в виде предмета. Понимание вещи в римском праве определяется материальной составляющей предмета, а также фактурой

---

[1] См.: Корпеев, А.Г. О предмете преступлений, совершаемых с использованием информационно-телекоммуникационных сетей, по уголовному законодательству Российской Федерации и Туркменистана. Юридический аналитический журнал. 2023. 18 (1). С. 20-24.

[2] См.: Корпеев, А.Г. О предмете преступлений, совершаемых с использованием информационно-телекоммуникационных сетей, по уголовному законодательству Российской Федерации и Туркменистана. Юридический аналитический журнал. 2023. 18 (1). С. 20-24.

ценностного эквивалента, когда материально выраженная ценность имеет значимость.

Предметом преступления могут быть материальные блага, такие как вещи, ценности, которые имеют физическое воплощение. Предмет преступления являются объекты реального мира, которые отражены в уголовном законодательстве, с помощью которых осуществляется воздействие на общественные отношения[1].

При этом в уголовных учениях России и Туркменистана сформировалась научная концепция, по которой под предметом преступления подразумеваются различные составляющие окружающего мира ценностного характера, на которые совершается воздействие в ходе совершения противоправного посягательства[2].

В этом контексте в уголовном законодательстве России и Туркменистана законодателем устанавливается ответственность «*по двум группам посягательств, предметом которых является информация: а) совокупность деяний, совершение которых направлено на уничтожение, модификацию, блокирование конкретных сведений (информации) (глава 28 УК РФ, глава 33 УК Туркменистана); б) совокупность нецифровых деяний, совершение которых направлено на завладение информацией неэлектрического происхождения (ст. 137, 276 УК РФ, 144, 151 УК Туркменистана)*[3]. *Вторая группа характеризуется отсутствием цифрового элемента в социально-правовой природе информации, т.е. данная информация*

---

[1] Наджафи, Г. М. Предмет компьютерных преступлений // Вестник Института законодательства Республики Казахстан, № 4. 2012. С. 125.

[2] См.: Корпеев, А.Г. О предмете преступлений, совершаемых с использованием информационно-телекоммуникационных сетей, по уголовному законодательству Российской Федерации и Туркменистана. Юридический аналитический журнал. 2023. 18 (1). С. 20-24.

[3] См.: См. Юрченко, И.А. Преступления против информационной безопасности: Учебное пособие / И.А. Юрченко — Москва : Проспект, 2021. Глава 5, С. 6. [Электронный ресурс]. URL: https://www.litres.ru/static/or4_adapters/view/or.html?baseurl=/download_book/69442084/100038685/&art=69442084&user=1187924154&uilang=ru&catalit2&track_reading&fb3_master=&fb3_master=2 (дата обращения 23.05.2025).

является видом материального воплощения, однако наличие основ электрического использования у нее нет»[1].

Информация, определяемая как охраняемая законом, исходя из логики закона не предоставляет возможности установить виды такой информации, соответственно затрудняется определение информации в качестве предмета компьютеризованных преступлений. Кроме того, нормативные правовые акты вовсе определяют информацию объектом правоотношений. «Информация может являться объектом публичных, гражданских и иных правовых отношений, она может свободно использоваться любым лицом и передаваться одним лицом другому лицу[2] (ст. 5 Федерального закона от 27.07.2006 № 149-ФЗ)»[3].

Однако мы считаем, что информацию следует определять предметом компьютеризованных преступлений: несмотря на свою нематериальность, информация – это ценность, и на нее могут воздействовать различными способами. Информация — на сегодняшний день это сверх ресурс, содержащий в себе совокупность важных сведений.

Следует согласиться с Е.А. Русскевичем в том, что «компьютерная информация по своей сути определяется как предмет посягательства, который выражен в сведениях, например, сообщения, данные, которые личность сознает при восприятии объекта посягательства»[4].

В этом смысле следует признать, что предмет преступлений в сфере компьютерной информации имеет широкое значение с учетом внедрения в жизнь большого количества электрических аппаратов, однако информация является центральным звеном данной цепочки, на которое оказывается

---

[1] Там же: Глава 5, С.6.

[2] Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149 –ФЗ. [Электронный ресурс]. URL.: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 21.01.2025).

[3] См. Корпеев, А.Г. О предмете преступлений, совершаемых с использованием информационно-телекоммуникационных сетей, по уголовному законодательству Российской Федерации и Туркменистана. Юридический аналитический журнал. 2023. 18 (1): 20-24.

[4] См. Русскевич, Е.А. Компьютерные преступления: квалификационные алгоритмы и тренды: учебное пособие. Москва: Проспект, 2025. 120 с.

воздействие в процессе возникновения общественных отношений с противоправным толком. Условия нематериальности тут не имеют значения, главным фактором является ценность такой информации.

Изменение уклада жизни в сфере информационных отношений выводит уголовно-правовое понимание предмета в части преступлений в сфере компьютерной информации на новый уровень понимания.

Исходя из этого, предметами преступлений в сфере компьютерной информации могут являться различные физические объекты, имеющие вещное воплощение, при этом, как определено выше, предметом также является информация, представленная в виде многообразия сведений цифрового характера. По смыслу главы 28 УК РФ и главы 33 «Преступления в сфере информатики и связи» УК Туркменистана предметами таких преступлений следует также признавать: информацию и (или) национальную критическую информационную инфраструктуру[1].

Способы совершения.

Важной особенностью преступлений в сфере компьютерной информации являются способы совершения таких преступлений. Вообще специфика компьютезированных преступлений зачастую приводят к полемике в уголовно-правовой науке о содержании способов совершения преступлений.

Замысел деяния предполагает под собой целый набор мыслительных действий для сокрытия преступного посягательства. Преступник не хочет быть пойман, а это значит, что способ должен быть универсальным. В этом плане компьютерные преступления являются как раз такими видами преступлений, которые предлагают широкий перечень различных универсальных способов совершения преступления.

---

[1] См.: Корпеев А.Г. О предмете преступлений, совершаемых с использованием информационно-телекоммуникационных сетей, по уголовному законодательству Российской Федерации и Туркменистана // Юридический аналитический журнал. 2023. 18 (1). С. 20-24.

Способы преступлений, предусмотренных ст. 272-274[3] УК РФ и 373-383 УК Туркменистана, образуют некоторые виды манипуляций в сфере компьютерной информации, которыми является: 1) незаконный доступ / неправомерный доступ – проникновение в электрическую систему любого устройства, а также информационную систему, в которой содержится информация (272 УК РФ и 373 УК Туркменистана); 2) принуждение к передаче информации – умышленное применение физических и моральных форм насилия с целью завладения информацией (374 УК Туркменистана), 3) уничтожение – действия, направленные на уничтожение информации (272 УК РФ, 375 УК Туркменистана), 4)изменение (формулировка в УК Туркменистана /модификация (формулировка в УК РФ) – процесс изменения первоначального вида информации путем внесения корректировок (272 УК РФ, 375 УК Туркменистана), 5)копирование – операция по созданию дубликата информации (272 УК РФ, 377 УК Туркменистана), 6)нарушение нормальной работы (такую формулировку предлагает УК Туркменистана) / неправомерное воздействие (такую формулировку предлагает УК РФ, но данные формулировки имеют одно значение) – постороннее вмешательство в деятельность объектов системы информационного обеспечения и информационных сетей (376 УК Туркменистана, 274[1] УК РФ), 7) создание/использование/распространение – последовательный этап разработки программного обеспечения с вредоносным содержанием с целью нарушения работы информационной системы, а также завладения сведениями, представленные в форме цифровой информации (379 УК Туркменистана, 273 УК РФ).

Как мы видим, перечень способов совершения компьютерных преступлений широкий. С учетом сравнительно-правовой модели в УК Туркменистана и УК РФ можно обратить внимание на различную формулировку способов, но, конечно, это не коим образом не усугубляет

уголовно-правовое понимание способов, так как по своему лексическому значению эти формулировки являются идентичными.

Перечень таких способов неисчерпаемый, например, в уголовно-правовой науке выделяют и два других способа совершения: применением удаленного доступа и непосредственного доступа[1]. В данном случае мы считаем, что удалённый доступ — это не способ совершения преступления, а технический прием. Вместе с тем совершение преступления удаленным доступом следует отнести к элементу факультативных признаков объективной стороны – к месту совершения преступления.

Другим способом совершения также называют манипуляцию данными, однако точного раскрытия понятия не представлено. По нашему мнению, манипуляция данными – это воздействие на данные, в том числе ввод информации, изменение ее, блокировка, однако манипуляция данными является собирательным концептуальным значением, в который входят все нами выше перечисленные способы. Операционная составляющая манипуляции включает в себя все виды воздействия на информацию, а также обращения с ней.

Исходя из вышеизложенного следует определить правовую природу выделенных семи способов совершения преступлений по УК РФ и УК Туркменистана.

Неправомерный доступ – это завладение лицом, не имеющим разрешительных полномочий, информацией, без предоставленного согласия правообладателя данной информации.

Согласно материалам дела № 1-124/22, обвиняемый А., обладающий специальными познаниями в компьютерной технике, исполняя обязанности программиста ООО «Меркурий», без заключения трудового договора путем неправомерного доступа на сервер компании присвоил себе данные,

---

[1] Россинская Е.Р., Рядовский, И.А. Современные способы компьютерных преступлений и закономерности их реализации. Lex russica. 2019. С. 95-96.

являющиеся имуществом компании. Симоновским судом г. Москва действия лица были квалифицированы по ч. 1 ст. 272 УК РФ[1].

Второй способ – принуждение к передаче информации. Под ним понимается осуществление действий психического или физического принуждения на лицо, являющееся правообладателем информации, с целью завладения чужим имуществом/информацией. Стоит отметить, что такого способа совершения преступлений в сфере компьютерной информации не предусмотрено в УК РФ.

Третьим способом совершения преступления является уничтожение (в данном случае уничтожение информации) – под последним следует понимать приведение информации в состояние, когда она теряет свои свойства программного существования на электронных носителях. Часто уничтожение путают с удалением, однако стоит отметить, что это две разные функции, основным их отличительным свойством является степень ущерба. Так, при удалении информации последняя не теряет свойств существования, так как имеются алгоритмы по восстановлению такой информации (к примеру, лицо закрыло документ на компьютере, предварительно не сохранив документ после внесения туда данных, однако специальные программные возможности позволяют восстановить информацию в том виде, в котором она была до закрытия документа).

М.А. Ефремова под уничтожением информации понимает «…утрату возможности ее дальнейшего использования»[2]. Однако в любом случае и при любом восприятии понятия важен конечный итог существования информации на носителе и как раз в этом заключается различие понятий уничтожения и удаления.

---

[1] Приговор Симоновского суда г. Москвы, от 18 мая 2022 № 1-124/22. [Электронный ресурс]. URL: https://mos-gorsud.ru/rs/simonovskij/cases/docs/co (дата обращения: 07.02.2025)

[2] Ефремова, М.А. Уголовно-правовая охрана информационной безопасности: дисс. … док. юрид. наук: 12.00.08. М. 2017. С.339.

Четвертый способ изменения / модификации – несанкционированное изменение исходной структуры информации, путем внесения с помощью определенных алгоритмов преобразования подлинной информации. Стоит указать на различное наименование такого способа в УК Туркменистана и в УК РФ. При этом смысловое значение действия не имеет противоречий. Слово «изменение» является синонимом слова «модификация». Согласно толкованию, модификация — это видоизменение чего-либо, потеря подлинного вида, а что касается информации, то ее модификация – это изменение исходного кода[1].

Так, судом Чкаловского районного суда г. Екатеринбург по делу № 1-609/2017 Ж., имеющий навыки использования компьютерной информации, не имеющий оснований доступа к компьютерной информации Корпорации «К***», с применением электрических носителей, проник в машинный носитель информации и осуществил копирование информации, а также с помощью программного обеспечения модифицировал информацию, содержащуюся на машинном носителе. Суд квалифицировал деяние по ч.2 ст. 272 УК РФ[2].

Пятый способ совершения преступлений – копирование информации, т.е. создание копии информации посредством перемещения цифровых данных с одного электронного носителя на другой или посредством воспроизведения копии сведений в материальную форму (к таким относятся фотографирование, перенос информации на бумажный носитель путем распечатывания, воспроизведение информации на иных технических устройствах). Зачастую копирование информации, осуществляется лицами, имеющими доступ к такой

---

[1] См. Письмо Минцифры России от 27.01.2022 № П11-2-05-200-3571 О рассмотрении обращений субъектов предпринимательской деятельности и заинтересованных лиц в сфере информационных технологий. [Электронный ресурс]. URL.: https://www.consultant.ru/document/cons_doc_LAW_408074/ (дата обращения: 07.02.2025).

[2] Приговор Чкаловского районного суда г. Екатеринбург, от 07 августа 2017 года № 1-609/17. [Электронный ресурс]. URL.: https://sud-praktika.cloud/precedent/420329.html (дата обращения: 07.02.2025).

информации (с использованием своего служебного положения), с целью получения вознаграждения, а также путем злоупотребления доверием.

Исходя из материалов дела Коптевского районного суда г. Москвы № 1-121/18 установлено, что П. был назначен на основании приказа специалистом по консультированию клиентов и продаже оборудования в компании ПАО «***-Коммуникации», при этом согласно условиям трудового договора, П. принял на себя обязательства о нераспространении информации, являющейся коммерческой тайной, установленной локальными нормативными актами компании. Однако П, воспользовавшийся компьютерным устройством компании перенес (скопировал) с этого компьютерного устройства на электронный носитель, принадлежащий ему, информацию клиентов, обсуживающихся в корпорации. Судом действия лица были квалифицированы по ч.1 ст. 272 УК РФ[1].

Шестым способом преступлений в сфере компьютерной информации является нарушение нормальной работы (интерпретация в УК Туркменистана) /неправомерное воздействие (интерпретация в УК РФ) в обоих случаях действие направленно против критической информационной инфраструктуры, информационной системы предприятия, государства. Действия, описанные в разной интерпретации равнозначны по фонетическому смыслу, в обеих случаях имеется ввиду противоправное воздействие на критическую информационную инфраструктуру.

В п. 13 постановления Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37 под вышеуказанным действием понимается незаконное воздействие на критическую информационную структуру путем внедрения компьютерной программы либо компьютерной информации. Такое вмешательство может произойти путем внедрения

---

[1] Приговор Коптевского районного суда г. Москвы, от 06 июня 2018 года № 1-121/18. [Электронный ресурс]. URL: https://www.mos-gorsud.ru/rs/koptevskij/cases/docs/content/91bfdfc4-165b-4117-8220-0f8f14564101 (дата обращения: 07.02.2025).

вредоносной компьютерной программы в систему, являющуюся критической инфраструктурой. При этом определение «критическая» в данном случае означает важный стратегический объект для предприятия, государства с учетом экономических, социальных и иных интересов. Таких инцидентов в наше время огромное количество. Некоторые из них удается преодолеть с помощью защитной информационной инфраструктуры, а некоторые наносят сильный ущерб критической инфраструктуре.

Так, например, из истории громких информационных атак можно вспомнить инцидент с сибирским нефтяным проводом. Еще в 80-егоды прошлого столетия была совершена крупнейшая кибератака на критическую инфраструктуру Российской Федерации (тогда СССР), когда злоумышленники с помощью применения трояна проникли в систему управления нефтяным проводом, что привело к бесконтрольному увеличению подачи газа, а в последствии к взрыву нефтяного провода[1].

Следует отметить, что при совершении деяния злоумышленниками могут применяться сразу несколько способов совершения, иными словами последовательно исходя из умысла. Применение нескольких способов является весьма релевантным обстоятельством на пути к достижению противоправного умысла. Примером может являться случай, который произошел в 1994 году в США, когда преступник Д. взломал систему компании S.R.P и получил доступ к сведениям этой компании, часть из которых он уничтожил. Вместе с тем наряду с первым действием он скопировал персональные данные работников компании, а также финансовые данные, которые являются конфиденциальными[2]. Исходя из этого Д. было применено два способа совершения преступления: уничтожение информации и копирование информации.

---

[1] См.: Самые громкие кибератаки на критические инфраструктуры. [Электронный ресурс]. URL: https://habr.com/ru/companies/panda/articles/316500/ (дата обращения: 10.02.2025).
[2] См.: Там же.

Конгломерат способов совершения преступления является весьма широким с учетом возможностей информационно-технической составляющей, но сегодняшнее содержание уголовного законодательства Российской Федерации и Туркменистана имеет ограниченный круг способов, но при этом являющийся открытым к стремительному изменению информационно – технологических отношений. При всем при этом в уголовном законодательстве Российской Федерации и Туркменистана существует ряд сходных способов совершения преступления, но также имеются и специфичные для уголовного законодательства способы, выявляются и различные интерпретации таких способов, которые унифицированное значение. Но не смотря на объем содержания этих способов, на сегодняшний день они передают всю существенную сторону преступлений, представленных в уголовном законодательстве двух стран.

Средства совершения преступлений[1].

Другой важной составляющей объективной стороной преступлений в сфере компьютерной информации являются средства совершения таких деяний.

В уголовно-правовой науке под средством совершения преступлений понимается материальный компонент, иными словами материальная вещь в физическом воплощении, с помощью которой достигается преступный умысел[2].

Правовая природа использования различных средств совершения преступлений заключается в упрощении совершения преступного посягательства[3].

---

[1] См: Корпеев, А.Г. Средства совершения преступлений в сфере компьютерной информации по уголовному законодательству Российской Федерации и Туркменистана // Юридический вестник Самарского университета Juridical Journal of Samara University. 2025. Т. 11, № 2. С. 96-102.

[2] См.: Григорян Г.Р. Мошенничество в сфере компьютерной информации: проблемы криминализации, законодательной регламентации и квалификации: диссертация ... кандидата Юридических наук: 12.00.08. Самара, 2021. С. 128.

[3] См.: Уголовное право. Общая часть: Учебник. Издание второе переработанное и дополненное / Под ред. доктора юридических наук, профессора Л.В. Иногамовой-Хегай, доктора юридических наук, профессора А.И.

Исходя из технической особенности преступлений в сфере компьютерной информации правовая природа средств совершения таких видов деликтов заключается в применении наряду с материальными компонентами мира нематериальных компонентов[1].

Действительно правовая природа вышеуказанных деликтов предусматривает наличие нематериальных средств совершения преступлений, например, программное обеспечение, электронные сети, ведь по фактическим обстоятельствам данные компоненты информационных технологий являются инструментом для достижения противоправного умысла в сфере информационной безопасности. Другое обстоятельство заключается в функциональных особенностях вышеуказанных технологий, так как для передачи информации по сетям связи и для установки программного обеспечения нужен автоматизированный носитель, а именно электронно-вычислительная машина, которая является носителем программного обеспечения и инструментом ввода информации для последующей ее передачи по средствам связи.

В этом плане преступление совершается с помощью ввода вредоносной программы (ст. 273 УК РФ и ст. 379 УК Туркменистана), однако важной составляющей на пути реализации замысла является устройство, которое позволит совершить деяние. В связи с этим образуется цепь информационных технологий, которая порождает цепную реакцию в случае противоправного посягательства. Такая цепь выглядит как «дуэт» информационных технологий или цифровых средств совершения преступлений, связанных друг с другом как основной и вспомогательный элемент (устройство/электронный носитель/ программное обеспечение), (устройство/электронный носитель / информационно-телекоммуникационная

Рарога, доктора юридических наук, профессора А.И. Чучаева. — М.: Юридическая фирма «КОНТРАКТ»: ИНФРА-М, 2008. — 560 с.

[1] Корпеев, А.Г. Средства совершения преступлений в сфере компьютерной информации по уголовному законодательству Российской Федерации и Туркменистана // Юридический вестник Самарского университета Juridical Journal of Samara University. 2025. Т. 11, № 2. С. 96-102.

сеть). Поэтому формируется комплекс взаимосвязанных средств совершения преступления для реализации преступного умысла[1].

При этом условно рассматривая материальную и нематериальне. концепцию в отношении средств компьютерных преступлений, логично было бы разделить их исходя из вышеуказанного концептуального состояния (материальные и нематериальные).

Следует заметить, что преступления в сфере компьютерной информации (глава 28 УК РФ, 33 УК Туркменистана) являются по правовой природе бланкетными нормами. В связи с этим при определении таких средств следует руководствоваться действующим законодательством Российской Федерации и Туркменистана, регулирующим общественные отношения в сфере безопасности информации. Данная позиция подтверждается также постановлением Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37[2].

В законодательстве Туркменистана на этот счет представлен целый комплекс потенциальных средств совершения преступлений, имеющих ряд существенных особенностей, объясняющих природой их происхождения. Закон Туркменистана «О правовом регулировании развития сети Интернет и оказания интернет-услуг в Туркменистане» от 20 декабря 2014 г. в своих положениях рассматривает несколько видов технических устройств: а) электронно-вычислительные машины, б) информационно-телекоммуникационные сети, в) иные электрические носители[3]. В положениях

---

[1] Корпеев, А.Г. Средства совершения преступлений в сфере компьютерной информации по уголовному законодательству Российской Федерации и Туркменистана // Юридический вестник Самарского университета Juridical Journal of Samara University. 2025. Т. 11, № 2. С. 96-102.

[2] Постановление Пленума Верховного Суда РФ от 15.12.2022 N 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет». [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_434573/. (дата обращения: 21.08.2024).

[3] Закон Туркменистана «О правовом регулировании развития сети Интернет и оказания интернет – услуг в Туркменистане» от 20.12.2014 № 159-V. [Электронный ресурс]. URL: https://www.parahat.info/law/2014-12-29-zakon-turkmenistana-o-pravovom-regulirovanii-razvitiya-seti-internet-i-okazaniya-internet-uslug-v-turkmenistane (дата обращения: 22.10.2024).

Главы XXXIII «Преступления в сфере информатики и связи» (ст. 381 УК Туркменистана) к средствам совершения преступлений относятся программы, обеспечивающие шифровку информации, так называемые криптографические устройства защиты[1].

В Законе Туркменистана от 3 мая 2014 г. № 72-V «Об информации и ее защите» средства совершения преступлений рассматриваются под общей призмой различных информационных технологий, перечень которых является открытым, однако к таким исходя из положений следует отнести компьютерные устройства и коммуникационные средства[2].

Согласно положениям постановления Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37 к компьютерным устройствам относят ноутбуки, компьютеры, смартфоны, а также иные электронно-вычислительные устройства[3].

С другой стороны, средства совершения компьютерных преступлений можно классифицировать исходя из функциональных особенностей: устройства введения информации (планшеты, компьютерные мыши, клавиатура, сенсорные девайсы), устройства извлечения информации (принтеры, сканеры, девайсы с функцией воспроизведения звука), устройства, обеспечивающие хранение (жесткие диски, карты памяти, флеш-карты, оптические диски, магнитные диски)[4]. В совокупности три данных вида устройств являются носителями информации с материальной составляющей и

---

[1] Уголовный Кодекс Туркменистана от 12 июня 1997 № 222-I. [Электронный ресурс]. URL: online.zakon.kz/Document/? Doc_id=3129586 (дата обращения: 21.07.2024).

[2] Закон Туркменистана «Об информации и ее защите» от 3 мая 2014 года № 72-V. [Электронный ресурс]. URL: https://base.spinform.ru/show_doc.fwx?rgn=85142 (дата обращения: 29.01.2025).

[3] Постановление Пленума Верховного Суда РФ от 15.12.2022 N 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет». [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_434573/. (дата обращения: 21.08.2024).

[4] См.: Павлов, В.А. П12. Периферийные устройства ЭВМ Учебное пособие: Часть 1. СарФТИ, Саров, 2001. - 231 с.

образуют внутриродовую триаду видов вспомогательных средств при реализации противоправного умысла[1].

Другая категоризация средств совершения компьютерных преступлений рассматривается исходя из составных частей, образующих единое электрическое устройство к таким относятся внутренние аппаратные устройства (компьютерные процессоры, устройства оперативной памяти, игровые карты), внешние аппаратные устройства (это все внешние гаджеты, способствующие вводу информации в систему компьютерного устройства, выводу информации, а также распространению по средствам связи), универсальные периферийные средства обеспечения передачи информации (коммуникационные сети, сеть «Интернет», теле и радиостанции)[2]. Данная категоризация определяет несколько видов разнофункциональных устройств, в том числе средства передачи информации.

«*Классифицируются средства совершения преступлений также по своему производственному происхождению. К таким относят: средства, произведенные легальным способом, т.е. сертифицированные в стране использования устройства; другая группа средств относится к устройствам нелегального происхождения, т.е. когда устройства собраны, сконструированы подпольно, собственноручно, а равно кустарным способом*»[3].

Согласно подписанному соглашению между Правительством Российской Федерации и Правительством Туркменистана «О сотрудничестве в области обеспечения международной информационной безопасности» от 5 апреля 2019 г. фактором, негативно влияющим на международную информационную безопасность, является внедрение в общественную жизнь

---

[1] Корпеев, А.Г. Средства совершения преступлений в сфере компьютерной информации по уголовному законодательству Российской Федерации и Туркменистана // Юридический вестник Самарского университета Juridical Journal of Samara University. 2025. Т. 11, № 2. С. 96-102.

[2] См.: Крылов, А. Б. К 85 Устройство персонального компьютера : учеб.-метод. пособие/ А. Б. Крылов, М. А. Шеламова. – Мн.: БГМУ, 2006. – 62 с.

[3] См.: Поляков В.В., Лапин С.А. Средства совершения компьютерных преступлений// Доклады ТУСУРа, № 2 (32), 2014. С. 163

информационно-коммуникационных технологий[1]. При этом конкретный перечень таких технологий не приводится в двухстороннем соглашении. Вместе с тем в совокупную структуру технологий информационного характера, по нашему мнению, входят все устройства, правовая природа которых имеет цифровую основу (в частности аппаратные, программные устройства)[2].

Международные нормативные правовые акты, в частности в Конвенции о киберпреступлениях от 23 ноября 2001 г., также не приводится перечень средств совершения компьютерных преступлений: основной термин либо собирательный термин, который используется в Конвенции, - это «автоматизированные устройства»[3].

Отсутствие конкретного перечня таких устройств объясняется множественностью разновидностей таких средств в природе, к тому же невозможно определить конкретный перечень, так как степень развития автоматизированных электрических устройств увеличивается в прогрессии. Мы назвали такой эффект пространственно-временным континуумом, в описании которого лежит непрерывная реальность, именно с такой непрерывной силой в реальности появляются потенциальные средства совершения преступлений, включая их нематериальную составляющую[4].

Так, по материалам дела Комитерновского районного суда г. Воронежа, подсудимый А.Н. совершил распространение вредоносных программ с целью уничтожения компьютерной информации. Действия А.Н. были

---

[1] Соглашение между Правительством Российской Федерации и Правительством Туркменистана «О сотрудничестве в области обеспечения международной информационной безопасности» от 05.04.2019. [Электронный ресурс].URL.:https://www.mid.ru/ru/foreign_policy/international_contracts/international_contracts/2_contract/56086/ (дата обращения: 11.02.2025).

[2] Корпеев, А.Г. Средства совершения преступлений в сфере компьютерной информации по уголовному законодательству Российской Федерации и Туркменистана // Юридический вестник Самарского университета Juridical Journal of Samara University. 2025. Т. 11, № 2. С. 96-102.

[3] Конвенция о преступности в сфере компьютерной информации от 23 ноября 2001 года ETS № 185 //ЭПС «Система ГАРАНТ». . [Электронный ресурс]. URL: http://base.garant.ru/4089723/#ixzz5WwK9w8it (дата обращения: 13.08.2023).

[4] Корпеев, А.Г. Средства совершения преступлений в сфере компьютерной информации по уголовному законодательству Российской Федерации и Туркменистана // Юридический вестник Самарского университета Juridical Journal of Samara University. 2025. Т. 11, № 2. С. 96-102.

квалифицированы по ч. 3 ст. 273 УК РФ. В данном случае мы видим использование компьютерной программы как средства совершения посягательства[1].

Существует также решение Заельцовского районного суда г. Новосибирск, исходя из материалов дела гражданин осуществил неправомерный доступ к охраняемой законом информации, используя персональный компьютер с доступом к программному обеспечения компании, работником которой он являлся. Действия И.А. были квалифицированы по ч.2 ст. 272 УК РФ[2].

Вместе с тем Центральный районный суд г. Челябинск рассматривал уголовное дело в отношении А.Б. По материалам дела, А.Б., используя персональный компьютер с установленным жестким диском, подключенным к системе компании, осуществил неправомерный доступ к компьютерной информации. Действия А.Б. квалифицированы по ч. 3.ст. 272 УК РФ[3].

Исходя из совокупности представленных классификаций, можно отметить универсальность компьютерных преступлений, которая заключается в многогранной и безграничной природе средств совершения таких деяний. В этом смысле предлагаем выделить несколько важных групп средств совершения преступлений в сфере компьютерной информации: *компьютерные устройства* (частью данной группы являются персональные компьютеры и иные разновидности компьютеров, планшеты, игровые консоли и т.д.), *коммуникационные сети* (системы связи и передачи информации, ярким примером данной группы является сеть «Интернет»), вредоносное *программное обеспечение* (софт, состоящий из алгоритмов кодов, с помощью

---

[1] Приговор Коминтерновского районного суда г. Воронеж от 27.04.2017 № 1-271-2015. [Электронный ресурс]. URL: https://sud-praktika.cloud/precedent/546205.html (дата обращения: 11.02.2025).
[2] Приговор Заельцовского районного суда г. Новосибирск от 11.07.2017 № 1-283-2017. [Электронный ресурс]. URL: https://sud-praktika.cloud/precedent/339721.html (дата обращения: 11.02.2025).
[3] Приговор Центрального районного суда г. Челябинск от 27.02.2017 № 1-141/2017. [Электронный ресурс]. URL.: https://sud-praktika.cloud/precedent/256261.html (дата обращения: 11.02.2025).

которого управляется компьютерное устройство, к таким следует относить, вирусы, троянские программы, ботнеты)[1].

Выделенная «триада» средств совершения преступлений имеет общую концепцию существования, такие средства связаны между собой, а зачастую применяются в паре как основное и вспомогательное средство. В этом смысле целевое предназначение данных средств заключается в применении их как вспомогательных средств для реализации противоправного умысла. Кроме того, нужно сказать, что универсальность компьютерных преступлений также заключается в том, что без применения таких средств практически невозможно реализовать такой умысел. В этом смысле communis finis (общая цель) применения таких средств упирается в то, что, с одной стороны, такие средства упрощают человеческую жизнь, но с другой стороны, становятся потенциальными инструментами на пути злого умысла. Средства совершения преступлений в сфере компьютерной информации являются diverse (разнообразными). Исходя из этого понимание средств совершения преступлений в сфере компьютерной информации в Российской Федерации и Туркменистане имеет логически выстроенную общность, однако следует сказать, что с развитием уголовного законодательства двух стран сущностное понимание и перечень таких средств по умолчанию будет уточняться[2].

Объективная сторона.

Объективная сторона — это всегда совокупность внешних признаков субъекта. Описание объективной стороны в уголовно-правовых нормах происходит по-разному: бывает так, что в смысловой актив диспозиции заложена объективная сторона, но существуют нормы, в диспозиции которых содержится отсылка к той или иной норме с целью уточнения объективной стороны преступления, в данном случае имеет место бланкетный характер

---

[1] Корпеев, А.Г. Средства совершения преступлений в сфере компьютерной информации по уголовному законодательству Российской Федерации и Туркменистана // Юридический вестник Самарского университета Juridical Journal of Samara University. 2025. Т. 11, № 2. С. 96-102.

[2] См. там же.

нормы. Компьютеризованные преступления как раз-таки относятся к группе вышеуказанных деяний.

Основная задача в выявлении объективной стороны – это трактование уголовно-правового запрета, а именно действия или бездействия, которое в уголовно-правовом смысле подпадает под категорию преступных. В этом смысле объективная сторона преступления характеризуется совокупностью взаимодополняющих обстоятельств, определяющих наличие преступности в совершенном действие.

Описанные в Уголовных кодексах Российской Федерации и Туркменистана составы преступлений отражают широкий спектр возможных способов и методов, которые могут быть использованы для нарушения не только личных прав и интересов отдельных граждан, а также государственных интересов в сфере использования компьютерной информации.

«Каждый составной элемент объективных признаков (объект, объективная сторона) преступлений в сфере компьютерной информации, а равно и других составов преступлений уголовно-правового порядка, всегда определяются наличием ряда обязательных и факультативных признаков»[1].

«Особо важный компонент объективной стороны, отнесенный к категории обязательных признаков, в данном случае определяется как преступное деяние». Вместе с тем обязательным признаком являются последствия преступного деяния, например, уничтожение, блокирование и копирование компьютерной информации»[2].

Преступные последствия, а также их предметно-понятийное содержание достаточно подробно и детально рассмотрены в диспозиции преступлений, предусмотренных главой 28 УК РФ и главой 33 УК Туркменистана.

---

[1] См. Шахрай, С.С. Объективные и субъективные признаки в обще понятии состава преступлений в сфере компьютерной информации // Вестник Академии экономической безопасности МВД России. № 10. 2010. С. 133-134.

[2] Там же. С. 135

Уголовный кодекс Туркменистана, например, имеет широкую базу последствий, которые причиняются в результате использования разнообразных технических средств. Например, *статьи 373-383 УК Туркменистана предусматривают как незаконный доступ к компьютерной информации, так и распространение заведомо ложной информации, а также использование вредоносных программ и модификацию БПЛА*[1]*. Также в УК Туркменистана предусмотрены отличные от УК РФ деяния: ст. 374 «Принуждение к передаче информации», ст. 381 «Оказание услуг по размещению интернет-ресурсов, преследующих незаконные цели», ст. 382 «Неправомерное изменение идентификационного кода абонентского устройства сотовой связи, устройства идентификации абонента, а также создание, использование, распространение программ для изменения идентификационного кода абонентского устройства»*[2].

«Вместе с тем ключевым компонентом объективной стороны является установление связующей линии между самим действием и совокупностью последствий и/ или последствия – в уголовно правовой науке такой феномен обозначается причина-следственная связь. Причинно-следственную связь можно обнаружить в конструкционных элементах составов. Терминологический ряд обеспечивающий связку между действием и последствием (причинно-следственной связью) является ряд узконаправленных терминологических фраз, например, «повлекло» (указанное в статье 272 УК РФ, 375 УК Туркменистана, 373 УК Туркменистана), «заведомо предназначенных» (указанное в статье 273 УК РФ), «заведомо

---

[1] Уголовный кодекс Туркменистана от 12.06.1997 № 222-I в ред. от 29.09.2023. Газета Нейтральный Туркменистан. [Электронный ресурс]. URL: https://metbugat.gov.tm/newspaper?id=8291 (дата обращения: 27.10.2023).

[2] Уголовный кодекс Туркменистана от 12.06.1997 № 222-I в ред. от 29.09.2023. Газета Нейтральный Туркменистан. [Электронный ресурс]. URL: https://metbugat.gov.tm/newspaper?id=8291 (дата обращения: 27.10.2023).

сфальсифицированной» (указанное в ст. 378 УК Туркменистана), «преднамеренное использование» (указанное в ст. 379 УК Туркменистана)»[1].

Установление причино-следственной связи является фундаментальным основанием при квалификации таких видов деяния. К примеру, если вредоносная программа была создана и использована с целью уничтожения, блокирования или модификации компьютерной информации (273 УК РФ, 379 УК Туркменистана), в этом контексте создание, распространение данной программы является преступным актом; или же осуществлён неправомерный доступ к такой информации не со стороны законного владельца, а со стороны лица, не имеющего право осуществлять обработку информации (272 УК РФ, 377 УК Туркменистана).

В этом контексте Генеральная Прокуратура Российской Федерации в своих методических рекомендациях от 30 мая 2014 года определила сущность действия объективной стороны «неправомерный доступ к компьютерной информации». Согласно этой позиции, «под данным термином следует понимать любые действия, которые могут быть квалифицированы как незаконные или совершённые без соответствующего разрешения от правообладателя, в данном случае – от собственника или любого другого законного владельца информации. Это означает, что любое использование возможности получения доступа к компьютерной информации без разрешения от лица, обладающего правами на неё, считается неправомерным и может быть предметом уголовного преследования. При этом под доступом понимается проникновение в ее источник с использованием средств (вещественных и интеллектуальных) компьютерной техники, позволяющее

[1] Шахрай, С.С. Объективные и субъективные признаки в обще понятии состава преступлений в сфере компьютерной информации // Вестник Академии экономической безопасности МВД России. № 10. 2010. С. 136.

использовать полученную информацию (копировать, модифицировать, блокировать либо уничтожать ее)»[1].

Кроме того, по нашему мнению, одним из важных факультативных признаков объективной стороны, дополняющего обязательные признаки в плоскости рассматриваемых деяний, следует определять место совершения преступления. Вопрос определения места совершения компьютерных преступлений является спорным. На сегодняшний день определяется наличие двух концепций о месте совершения преступлений - это место, совершения действий, указанных в объективной стороне, и место наступления последствий, входящих в объективную сторону преступления. Относя данный аспект к спорному моменту, проведено социологическое исследование, которое показала, что 64,8 % опрошенных респондентов считают местом совершения компьютерных преступлений – место наступления последствий[2]. Считаем, что следует согласиться с мнением респондентов, так как совершение компьютерных преступлений зачастую сопряжено с экстерриториальностью, в связи с этим для обеспечения защиты различных общественных отношений важно определять местом совершения компьютерных преступлений – место наступления последствий, указанных в объективной стороне преступления, в том числе с целью применение уголовного законодательства страны, в котором наступили различные последствия.

Согласно ст. 273 УК РФ и 387 УК Туркменистана создание, использование и распространение вредоносных компьютерных программ объективная сторона преступления выражается в действии, направленном на создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для

---

[1] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации. [Электронный ресурс]. URL: https://www.garant.ru/products/ipo/prime/doc/70542118/ (дата обращения: 18.03.2024)

[2] См.: вопрос № 6 Приложения 1 к диссертации.

несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации[1].

Согласно постановлению Пленума Верховного Суда Российской Федерации объективная сторона преступления, предусмотренного ст. 273 УК РФ, 387 УК Туркменистана, состоит в выполнении одного или нескольких перечисленных в этой статье действий, а именно: 1) создание вредоносных программ с целью уничтожения, блокирования и модификации компьютерной информации, 2) распространение вредоносных программ или специальных средств, содержащих данные программы, 3) использование вредоносных программ и специальных средств, содержащих данные программы[2].

Одной из особенностей объективной стороны преступлений в сфере компьютерной информации по уголовному законодательству Российской Федерации и Туркменистана является отнесение составов преступлений через призму их структурирования к бланкетному типу. Данная особенность определяет, что объективные признаки данных преступлений устанавливаются при помощи множественных отсылок к иным нормам либо нормативным правовым актам, которые регламентируют функционирующие особенности информационных технологий[3].

Тут следует согласиться с позицией А.В. Пелевиной относительно того, что «огромный массив нормативных паровых актов, к которым отсылают вышеуказанные составы, являются противоречивыми и несовершенными с

---

[1] Уголовный Кодекс Туркменистана от 12 июня 1997 № 222-I. [Электронный ресурс]. URL: online.zakon.kz/Document/? Doc_id=3129586 (дата обращения: 21.07.2024); Уголовный Кодекс РФ от 13 июня 1996 № 63-ФЗ. [Электронный ресурс]. URL.: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения 22.05.2024).

[2] Постановление Пленума Верховного Суда РФ от 15.12.2022 N 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет». [Электронный ресурс]. URL.: https://www.consultant.ru/document/cons_doc_LAW_434573/. (дата обращения: 21.08.2024).

[3] Там же.

точки зрения регламентации режима функционирования компьютерной техники, а также трудны в понимании из-за изобилия технических терминов»[1].

Действительно, массив нормативных правовых актов в сфере компьютерной техники, информационной безопасности с каждым годом увеличивается и содержит огромное количество специфических норм и понятийно-категориального аппарата, зачастую понятное узконаправленному специалисту, разбирающемуся в алгоритмах функционирования данной техники.

В контексте рассматриваемых преступлений следует определить, что оконченным преступление следует признавать с момента совершения противоправного способа, как в совокупности, так и единолично, при этом одним из обязательных факторов будут являться последствия любого категориального ряда (например, уничтожение, блокирование, модификация, копирование информации)[2].

В УК Туркменистана объективная сторона преступлений в сфере компьютерной информации выражена в различных деяниях, перечень таких деяний значительно шире чем в УК РФ. Преобразование и наполнение новыми составами преступлений произошло достаточно недавно, в 2022 г., до этого момента наполнение главы было идентично главе 28 УК РФ.

Объективная сторона ст. 373 УК Туркменистана выражена «в незаконном доступе к информации, в информационную сеть или информационно-телекоммуникационную сеть»[3]. В данном случае согласно Закону Туркменистана № 2 от 3 мая 2014 г. «Об информации и ее защите» «под информацией понимаются все сведения или сообщения в бумажном,

---

[1] Пелевина А.В., Общая характеристика преступлений в сфере компьютерной информации. Пробелы в российском законодательстве, 4, 2015. С. 210.

[2] Постановление Пленума Верховного Суда РФ от 15.12.2022 N 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет». [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_434573/. (дата обращения: 21.08.2024).

[3] Уголовный Кодекс Туркменистана от 12 июня 1997 № 222-I. [Электронный ресурс]. URL: online.zakon.kz/Document/? Doc_id=3129586 (дата обращения: 21.08.2024).

электронном или ином виде, независимо от способов поиска, обработки, хранения, передачи и распространения»[1].

При этом, по нашему мнению, в целях конкретизации объективной стороны данного деяния имеет смысл уточнить, что такая информация является «компьютерной». Статья 373 УК Туркменистана является бланкетной, исходя из этого для уточнения понятийных категорий следует обращаться к иным нормативным правовым актам, однако в законодательстве Туркменистана, как и в нормативных правовых актах Российской Федерации, отсутствует понятие, «информационная сеть», включенное в вышеуказанную статью. *Согласно военному энциклопедическому словарю под информационной сетью понимается «совокупность пространственно разнесенных компьютерных средств (ЭВМ, дисплеи, проекторы, табло и др.), терминальных средств связи (аппараты телеграфные, телефонные, факсимильные; телетайпы и др.) и передачи данных (абонентские пункты, удаленные мультиплексоры и др.), объединенных с помощью каналов различных видов наземно-космической связи (почтовой, электрической, телекодовой, видеокомпьютерной и др.) для переработки (поиска, преобразования, передачи, хранения и др.) специальной и (или) массовой информации»*[2]. Соответственно, для правильного толкования объективной стороны предлагаем под информационной сетью понимать совокупность компьютерных устройств, объединенных между собой каналами связи для передачи компьютерной информации.

Согласно ст. 374 УК Туркменистана объективная сторона преступления выражается в «принуждении к передаче информации»[3]. Следует отметить, что такого состава преступления нет в Уголовном кодексе Российской Федерации.

---

[1] Закон Туркменистана «Об информации и ее защите» от 3.05.2014 года № 72V. [Электронный ресурс]. URL: https://online.zakon.kz/Document/?doc_id=34731231 (дата обращения: 21.08.2024).

[2]Военный энциклопедический словарь. [Электронный ресурс]. URL: https://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=13179@morfDictionary (дата обращения: 21.08.2024).

[3] Уголовный Кодекс Туркменистана от 12 июня 1997 № 222-I. [Электронный ресурс]. URL: online.zakon.kz/Document/? Doc_id=3129586 (дата обращения: 21.08.2024).

Основным действием в данном случае является принуждение, т.е. умышленное моральное, физическое насилие в отношении лица, обладающего доступом к информации, с целью завладения охраняемой законом информацией. В данном случае момент осуществления действия, направленного на склонение лица к передаче информации, будет являться фактом совершения преступления, в данном случае центральное место в причинении общественно опасных последствий занимает принуждение, т.е. сам факт давления на лицо с целью завладения информацией[1].

Согласно ст. 375 УК Туркменистана объективной стороной данного деяния является «незаконное уничтожение информации или изменение ее формата»[2]. В контексте данного состава в объективную сторону преступления стоило бы добавить слово «копирование», так как информация может быть не только уничтожена или изменена, но и незаконно скопирована, в данном случае объективная сторона будет расширена в плане противоправных действий, но позволит криминализировать незаконное копирование и создать триаду общественно опасных последствий, важных с точки зрения оптимизации защиты компьютерной информации[3]. Также, по нашему мнению, следует обратить внимание на слово «изменение ее формата»: данную фразу следует заменить на «ее модификацию», так как компьютерная информация может быть не только изменена в формате, но могут быть измены ее свойства, целостность. В этом плане модификация – комплексное понятие, которое является инструментом противодействия любым изменениям компьютерной информации.

Принципиально важное значение в уголовном законодательстве Туркменистана придается безопасной работе информационно-

---

[1] Уголовный Кодекс Туркменистана от 12 июня 1997 № 222-I. [Электронный ресурс]. URL: online.zakon.kz/Document/? Doc_id=3129586 (дата обращения: 21.08.2024).
[2] Уголовный Кодекс Туркменистана от 12 июня 1997 № 222-I. [Электронный ресурс]. URL: online.zakon.kz/Document/? Doc_id=3129586 (дата обращения: 21.08.2024).
[3] Уголовный Кодекс Туркменистана от 12 июня 1997 № 222-I. [Электронный ресурс]. URL: online.zakon.kz/Document/? Doc_id=3129586 (дата обращения: 21.08.2024).

телекоммуникационных сетей и в целом информационной инфраструктуры. Это закреплено в ст. 376 УК Туркменистана, объективная сторона которой выражена «в нарушении нормальной работы информационной системы и информационно-телекоммуникационной сети»[1]. Согласно Закону Туркменистана от 3 мая 2014 г. № 72-V «Об информации и ее защите», под информационной системой понимается «совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств»[2]. Такое понятие является аналогичным понятию информационной системы, закрепленному в Федеральном законе Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Стоит обратить внимание на словосочетание «нормальная работы»: не совсем понятно, что понимается под нормальной работой, а также, по нашему мнению, корректно объективную сторону ст. 376 УК Туркменистана следует изменить следующим образом: «нарушение безопасности информационной системы и информационно-телекоммуникационных сетей». Под безопасностью информационной системы и информационно-телекоммуникационных сетей понимать нарушение процесса обработки и хранения информации с различным правовым режимом посредством несанкционированного вмешательства в их работу.

В ст. 377 УК Туркменистана объективная сторона выражена в «незаконном присвоении информации», а равно в умышленном копировании или присвоении иным способом охраняемой законом информации в информационной системе или проходящей через информационно-телекоммуникационную сеть[3]. Аналогии данной статьи в УК РФ нет.

---

[1] Уголовный Кодекс Туркменистана от 12 июня 1997 № 222-I. [Электронный ресурс]. URL: online.zakon.kz/Document/? Doc_id=3129586 (дата обращения: 21.08.2024).

[2] Закон Туркменистана от 3 мая 2014 года № 72-V. [Электронный ресурс]. URL: «Об информации и её защите» https://online.zakon.kz/Document/?doc_id=34731231.

[3] Уголовный Кодекс Туркменистана от 12 июня 1997 № 222-I. [Электронный ресурс]. URL: online.zakon.kz/Document/? Doc_id=3129586 (дата обращения: 21.08.2024).

Вызывает сомнение фразы, содержащейся в объективной стороне, «иным способом». Считаем, что следует данную фразу исключить, так как имеется широкий спектр способов завладения чужой информации, либо определенно закрепить способы незаконного копирования или присвоения информацией, что позволит оптимизировать подход правоприменителей в установлении обстоятельств нарушенного права.

Важной составляющей комплексной безопасности компьютерной информации являются меры, принимаемые в сфере защиты от вредоносных программ. Обширный конгломерат вредоносных программ на сегодняшний день умышленно разрабатываются и внедряются в компьютерную информационную структуру с целью причинения ущерба человеку, обществу и государству.

Еще в 1970-е годы прошлого столетия Джон Браннер *описывал компьютерный вирус и называл его «червем», в его книге «Оседлавшая волну шока» амбициозный программист, целью которого является изменение сложившегося мирового порядка, спасает мир от деспотического проявления, используя программное обеспечение «червь», которое распространяется по компьютерам, разрушая всю информацию, хранящуюся в них*[1].

Если для обывателя того времени такой сюжет казался нереалистичным, то сегодня разрушающая информацию программа – это не только реальность, но и проблема. Более половины преступлений в информационном пространстве совершается с фишинговых сообщений либо вредоносного приложения к сообщениям в электронной почте, мессенджерах. Уровень данных деяний варьируется от простых до сложных, все зависит от того, кто по ту сторону компьютера - обычный человек либо сотрудник государственной корпорации. Вредоносная программа является средством

[1] Предсказания фантастов, сбывшиеся в технологиях (Из книги Джона Браннера «Оседлавший волну шока». 1975). [Электронный ресурс]. URL: https://myatom.ru/metromozg/prognoz/ (дата обращения: 1.05.2025).

для поражения информационных ресурсов, например, веб-сайтов. Для начала злоумышленник взламывает сайты, вторым шагом, в случае успешного взлома, является внедрение вредоносного кода в структуру сайта с целью получения контроля и дальнейшего распространения вредоносного ПО.

В уголовном кодексе Туркменистана вредоносным программам посвящена статья 379 УК Туркменистана, практически аналогичная статье 273 УК РФ. Объективной стороной данного преступления является «создание, использование и распространение вредоносных программ», а преступление является оконченным с совершения одного из действий объективной стороны, т.е. создания, использования, распространения[1]. Усиливают общественную опасность закрепленные квалифицирующие признаки ч.2, касающиеся «ответственности за использование вредоносных программ в отношении источников национальной электронной информации, национальной информационной системы или критически важных объектов с использованием служебного положения»[2].

К тому же в УК Туркменистана содержится ряд специфических составов преступлений, которые не имеют аналогий в УК РФ. Ст. 380 УК Туркменистана незаконное распространение электронных источников информации, ст. 381 УК Туркменистана оказание услуг по размещению интернет-ресурсов, ст. 382 УК Туркменистана неправомерное изменение идентификационного кода абонентского устройства, ст. 383 УК Туркменистана умышленное нарушение требований технических измерений

---

[1] См.: Постановление Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» //СПС«КонсультантПлюс». [Электронный ресурс]. URL:https://www.consultant.ru/document/cons_doc_LAW_43457

[2] См.: Уторова, Т. Н. Преступления в сфере информационной безопасности : учебное пособие / Т. Н. Уторова, Л.А. Колпакова ; Министерство науки и высшего образования Российской Федерации, Московский государственный юридический университет имени О.Е. Кутафина (МГЮА), Северо-Западный институт (филиал) Университета имени О.Е. Кутафина (МГЮА). - Вологда : Северо-Западный ин-т (филиал) Ун-та им. О. Е. Кутафина (МГЮА), 2024. С.75; Уголовный Кодекс Туркменистана от 12 июня 1997 № 222-I. [Электронный ресурс]. URL: online.zakon.kz/Document/? Doc_id=3129586 (дата обращения: 21.08.2024); Уголовный Кодекс РФ от 13 июня 1996 № 63-ФЗ. [Электронный ресурс]. URL.: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения 22.05.2024).

БПЛА[1]– это отличительная особенность УК Туркменистана от УК РФ в части закрепления данных деяний в качестве составов преступлений[2].

Действительно, способы нанесения ущерба с помощью компьютерных технологий достаточно разнообразны. Данный тезис стал основой в формировании целой главы УК Туркменистана.

Определяя преступления в сфере компьютерной информации как бланкетные, следует отметить, что в Туркменистане, не смотря на многообразие преступных посягательств в сфере компьютерной информации на сегодняшний день не сформирована разъясняющая судебная практика в сфере совершения преступлений в сфере компьютерной информации. В связи с этим в заключении для конкретизации объективных признаков преступлений в сфере компьютерной информации по уголовному законодательству Туркменистана разработан первый проект постановления Верховного Суда Туркменистана (см. Приложение №2).

2.2. Специфика субъективных признаков преступлений в сфере компьютерной информации по современному уголовному законодательству России и Туркменистана[3]

Согласно уголовно-правовой науке состав преступления формируется из четырех важных элементов, образующих уголовно-правовую сущность совершенного деяния. Одним из таких элементов является субъект преступления и субъективная сторона.

Субъект[4].

---

[1] Уголовный Кодекс Туркменистана от 12 июня 1997 № 222-I. [Электронный ресурс]. URL: online.zakon.kz/Document/? Doc_id=3129586 (дата обращения: 21.08.2024).

[4] См.: Корпеев, А.Г. О субъекте преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (технологий), по уголовному законодательству Российской Федерации и Туркменистана / А. Г. Корпеев // Вопросы российского и международного права. – 2024. – Т. 14, № 1-1. С. 569-578

По общему правилу субъектом преступлений, предусмотренных уголовным законом, является вменяемое физическое лицо, достигшее 16 летнего возраста (ст. 19 УК РФ и УК Туркменистана)[1]. Вместе с тем уголовным законодательством двух стран по ряду преступлений предусмотрено наступление уголовной ответственности для субъектов, достигших возраста 14 лет[2].

Исходя из положений главы 28 УК РФ «Преступления в сфере компьютерной информации» и главы 33 УК Туркменистана «Преступления в сфере информатики и связи», субъектом таких деяний признается лицо, достигшее 16-летнего возраста[3]. Однако правовая природа компьютерных преступлений и специфика их совершения предполагает кроме наступления возраста уголовной ответственности и другие характеристики определения данного субъекта.

Специфика подходов к характеристике субъекта определяется множественностью. В рамках теории о преступлениях в сфере компьютерной информации сформировалась позиция, что субъектом преступления может быть не просто вменяемое лицо, достигшее возраста уголовной ответственности, но и лицо, способное стать полноценным субъектом информационных отношений. Другая позиция основывается на категоризации субъекта исходя из набора факультативных: общий и специальный (физическое лицо, имеющее определённые навыки, позволяющее совершить определённый вид преступлений)[4].

---

[1] Уголовный Кодекс Туркменистана от 12 июня 1997 № 222-I. [Электронный ресурс]. URL: online.zakon.kz/Document/? Doc_id=3129586 (дата обращения: 21.08.2024).

[2] Уголовный Кодекс Туркменистана от 12 июня 1997 № 222-I. [Электронный ресурс]. URL: online.zakon.kz/Document/? Doc_id=3129586 (дата обращения: 21.08.2024); Уголовный Кодекс РФ от 13 июня 1996 № 63-ФЗ // Собрание законодательства РФ. – 1996. – № 25.

[3] Уголовный Кодекс Туркменистана от 12 июня 1997 № 222-I. [Электронный ресурс]. URL: online.zakon.kz/Document/? Doc_id=3129586 (дата обращения: 21.08.2024); Уголовный Кодекс РФ от 13 июня 1996 № 63-ФЗ. [Электронный ресурс]. URL.: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения 22.05.2024). .

[4] Ефремова, М.А. Уголовная ответственность за преступления, совершаемые с использованием информационно-телекоммуникационных технологий. - М.: Юрлитинформ, 2015. С. 87.

К категории специальных видов субъектов относят лиц, соответствующих характеристике общего субъекта, но имеющих дополнительные функциональные возможности в сфере использования компьютерной информации: как сказано выше, лицо, достигшее 16-летнего возраста[1] и лицо с навыками в сфере информатики[2].

Картина факультативных признаков субъекта преступлений в сфере компьютерной информации исходя из «буквы закона» выражается в совершении особых действий: возможность доступа к компьютерной информации (ст. 272 и 274 УК РФ, ст. 373 и 375 УК Туркменистана); доступ к информационно-телекоммуникационным сетям (ст. 272 и 274 УК РФ, ст. 376 УК Туркменистана); доступ в критическую информационную систему (ст. 272 -274 УК РФ, ст. 376, 379 и 380 УК Туркменистана)[3].

Субъектом преступлений, предусмотренных ст. 272^1 УК РФ, ч.2 ст. 273 УК РФ, 274 УК РФ, 274^1 УК РФ, $274^{2,}$ является общий, однако в части 3 квалифицирующим признаком определяется использование служебного положения. Условно мы можем сказать, что, например, при квалификации преступления по ч. 3 ст. 272^1 следует устанавливать дополнительные факультативные признаки субъекта преступления, а именно определять должностной статус лица, полномочия, закрепленные за ним, а также правоустанавливающие документы на использование и обращение охраняемой законом информации.

Так, Промышленным районным судом г. Самары рассматривалось деяние, совершенное Ч. путем неправомерного доступа к компьютерной

---

[1] См.: Корпеев, А.Г. О субъекте преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (технологий), по уголовному законодательству Российской Федерации и Туркменистана / А. Г. Корпеев // Вопросы российского и международного права. – 2024. – Т. 14, № 1-1. С. 569-578.

[2] Ефремова, М.А. Уголовная ответственность за преступления, совершаемые с использованием информационно-телекоммуникационных технологий. - М.: Юрлитинформ, 2015. С. 87.

[3] Уголовный Кодекс Туркменистана от 12 июня 1997 № 222-I. [Электронный ресурс]. URL: online.zakon.kz/Document/? Doc_id=3129586 (дата обращения: 21.08.2024); Уголовный Кодекс РФ от 13 июня 1996 № 63-ФЗ. [Электронный ресурс]. URL.: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения 22.05.2024).

информации. Установлено, что Ч. был принят на работу в компанию посредством заключения трудового договора, а также оформления должностной инструкции, предусматривающих порядок обращения с конфиденциальной информацией компании, в которую входят персональные данные клиентов, включая абонентские номера, организации. Гражданин Ч., используя свое служебное положение, осуществил вход со своего персонального компьютера, подключенного к системе организации, в информационный реестр абонентских номеров клиентов организации, используя учетные данные лица (пароль и логин), выданные ему как продавцу-консультанту, обнаружил, что к абонентскому номеру привязан счет с денежными средствами в размере 30000 рублей. Реализуя преступное намерение, он вывел данные средства со счета клиента организации на свой собственный счет[1]. Как мы видим, судом установлен факт того, что лицо, используя свое служебное положение и имея доступ к корпоративной информации, в том числе к персональным данным клиентов, на основании таких документов, как трудовой договор, должностная инструкция, локальные нормативные акты организации, воспользовалось данным обстоятельством для реализации преступного умысла. При этом важен также факт доведения до лица его прав и обязанностей путем ознакомления с правоустанавливающими документами.

На этот счет в п.12 постановления Пленума Верховного Суда Российской Федерации № 37 от 15 декабря 2022 г., указывается, что до лица, на которое возложено соблюдение правил, регламентирующих обработку персональных данных, должна быть в императивном порядке доведена информация о соблюдении таких правил, и способами доведения такой информации как раз является факт подписания трудового договора, а также

[1] См.: Приговор Промышленного районного суда г. Самары № 1-87/2017 от 2017 года. [Электронный ресурс]. URL: https://sud-praktika.cloud/precedent/201301.html (дата обращения: 18.02.2025).

иных актов, предусматривающих работу с конфиденциальной информацией в информационной системе организации[1].

Что касается уголовного законодательства Туркменистана, тут следует отметить, что характеристика субъекта является аналогичной той, что существует в УК Российской Федерации, в частности в ст. 373, 374, 375, 378, 381, предусматривающих деяния, связанные с незаконным доступом к информации, с принуждением к передаче информации, распространение заведомо сфальсифицированной информации и предоставление услуг по размещению интернет-ресурсов[2]. Исходя из положений вышеуказанных преступлений, субъект характеризуется как общий субъект преступлений, т.е. лицо, достигшее возраста уголовной ответственности (16 лет). Условно также в некоторых конструкциях преступлений имеются и факультативные признаки характеристики субъекта, связанные с наличием служебных функций[3].

Анализируя основные постулаты уголовно-правовой науки Российской Федерации и Туркменистана в части сущности определения субъекта преступлений в сфере компьютерной информации следует отметить, что уголовное законодательство двух стран в преступлениях, предусмотренных главами 28 УК РФ и 33 УК Туркменистана, предусматривает по общим основаниям уголовно-правового регулирования в качестве субъекта преступления вменяемое физическое лицо, достигшее возраста уголовной ответственности. В Российской Федерации и Туркменистане это возраст - 16 лет[4].

---

[1] Постановление Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет». [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_434573/. (Дата обращения: 21.08.2024).

[2] Уголовный Кодекс Туркменистана от 12 июня 1997 № 222-I. [Электронный ресурс]. URL: online.zakon.kz/Document/? Doc_id=3129586 (дата обращения: 21.08.2024).

[3] Уголовный Кодекс Туркменистана от 12 июня 1997 № 222-I. [Электронный ресурс]. URL: online.zakon.kz/Document/? Doc_id=3129586 (дата обращения: 21.08.2024).

[4] Уголовный Кодекс Туркменистана от 12 июня 1997 № 222-I. [Электронный ресурс]. URL: online.zakon.kz/Document/? Doc_id=3129586 (дата обращения: 21.08.2024); Уголовный Кодекс РФ от 13 июня

При этом, учитывая специфику деятельности, связанной с использованием информационного пространства, а также средств информационных технологий, субъект преступлений в сфере компьютерной информации, предусмотренных уголовным законодательством Российской Федерации и Туркменистана, в частности ч.3 ст. 272[1], ч.3 ст. 273 УК РФ, ч.4 ст. 274[1] УК РФ, ч.2 ст. 378 УК Туркменистана, ч.2 ст.379 УК Туркменистана, ч. 2 ст. 380 УК Туркменистана, характеризуется дополнительным (факультативным) признаком, а именно использованием своего служебного положения[1].

Как было замечено ранее, в уголовно-правовой науке выделяют еще одну факультативную характеристику субъекта преступлений в сфере компьютерной информации, которая не предусмотрена уголовным законом Российской Федерации и Туркменистана. Речь идет о лице, обладающем навыками в сфере информатики. Следует отметить, что такая позиция является релевантной, так как использование компьютерного средства, а также совершение с его использованием различных действий в отношении компьютерной информации предполагает обладание определёнными навыками[2].

На этот счет стоит выделить ст. 273 УК РФ и 379 УК Туркменистана, связанные с созданием, использованием и распространением вредоносных программ, ведь не каждый человек обладает навыками по созданию и использованию вредоносного программного обеспечения[3]. В связи с этим не вызывает сомнения наличие дополнительного признака субъекта

1996 № 63-ФЗ. [Электронный ресурс]. URL.: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения 22.05.2024).

[1] См.: Корпеев, А.Г. О субъекте преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (технологий), по уголовному законодательству Российской Федерации и Туркменистана / А. Г. Корпеев // Вопросы российского и международного права. – 2024. – Т. 14, № 1-1. С. 569-578.

[2] См. Там же.

[3] Уголовный Кодекс Туркменистана от 12 июня 1997 № 222-I. [Электронный ресурс]. URL: online.zakon.kz/Document/? Doc_id=3129586 (дата обращения: 21.08.2024); Уголовный Кодекс РФ от 13 июня 1996 № 63-ФЗ. [Электронный ресурс]. URL.: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения 22.05.2024).

преступлений в сфере компьютерной информации – лицо, обладающее навыками в сфере информатики[1].

Исходя из этого следует определить, что на сегодняшний день субъекта преступлений в сфере компьютерной информации в рамках уголовного законодательства Российской Федерации и Туркменистана целесообразно определять по общему признаку: вменяемое физическое лицо, достигшее возраста уголовной ответственности (16 лет), а также в некоторых ситуациях с учетом дополнительных признаков: лицо, совершившее преступное деяние с использованием служебного положения; лицо, обладающее навыками в сфере информатики[2].

Субъективная сторона.

В контексте преступлений, предусмотренных ст. 272 УК РФ и 373 УК Туркменистана, - незаконный либо неправомерный доступ к компьютерной информации субъективная сторона выражается в форме умыла. Лицо совершаемое вышеуказанное деяние имеет все основания осознано воспринимать наступление общественно-опасных последствий. Вместе с тем объективной стороне данного вида деяние уже заложен субъективный компонент (неправомерный доступ), иными словами лицо осознает, что совокупность действий является неправомерными с точки зрения закона.

С.М Кочои и Д.Б. Савельев считают, что данные преступные акты совершаются с прямым умыслом. По сути лицо, совершающее неправомерный доступ в компьютерную систему, имеет все основания полагать с точки зрения определенных навыков владения техническими средствами, а также будучи ознакомленным с регламентами использования такой информации, что его

---

[1] См.: Корпеев, А.Г. О субъекте преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (технологий), по уголовному законодательству Российской Федерации и Туркменистана / А. Г. Корпеев // Вопросы российского и международного права. – 2024. – Т. 14, № 1-1. С. 569-578.

[2] См.: Корпеев, А.Г. О субъекте преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (технологий), по уголовному законодательству Российской Федерации и Туркменистана / А. Г. Корпеев // Вопросы российского и международного права. – 2024. – Т. 14, № 1-1. С. 569-578.

действия по своей сути являются незаконными. Проникновение в информационную систему с целью завладения сведениями электронного характера априори может рассматриваться только в рамках прямого умысла[1].

Тут следует согласиться с авторами, которые утверждают, что субъективную сторону ст. 272 УК РФ и 373 УК Туркменистана следует рассматривать через призму вины в форме умысла.

По нашему мнению, неосторожность в данном случае является нелогичным компонентом в совершении данных деяний, так как лицо всегда осознает степень дозволенного доступа к информации либо к информационной системе, т.к. обычно уровень разрешенности доступа к получению информации прописан локальным нормативным актом организации.

К примеру, Ленинским районным судом города Севастополя 18.09.2023 года вынесено решение по ч.3 ст. 272 УК РФ. Судом установлено, что сотрудник полиции А. вопреки установленным Федеральным законом «О персональных данных» от 27.07.2006 № 152-ФЗ правилам обращения с персональными данными, а также ч. 1 ст. 9 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», ч 4 и 7 ст. 17 Федерального закона от 07.02.2011 № 3-ФЗ «О полиции», приказу МВД России от 07.06.2013 № 369-дсп, утверждающему инструкцию о порядке эксплуатации программно-технического комплекса интегрированного банка данных коллективного пользования федерального уровня, а также контракту о прохождении службы в органах внутренних дел Российской Федерации, заключенному между сотрудником А. и уполномоченным начальником УМВД России по г. Севастополь, в соответствии с которым он обязан не разглашать охраняемую законом тайну, конфиденциальную информацию, по просьбе товарища о предоставлении

[1] Кочои С., Савельев Д. Ответственность за неправомерный доступ к компьютерной информации. Российская юстиция, 1999. [Электронный ресурс]. URL.: https://base.garant.ru/3540854/ (дата обращения 1.04.2024).

некоторых персональных данных, содержащихся в делах, имея доступ и заведомо зная о последствиях, передал второму интересующие того персональные данные. В связи с этим суд вынес решение признать сотрудника А. виновным по ч.3 ст. 272 и назначил наказание в виде штрафа в размере 40000 рублей, с лишением права занимать должности на государственной службе сроком на один год[1].

Октябрьским районным судом г. Ростова-на-Дону 15.09.2023 вынесено решение в отношении Б. по ч.3 ст. 272 УК РФ. Судом установлено, что гражданин был принят на работу в организацию на должность специалиста по клиентскому сервису направления обслуживания клиентов массового рынка в голосовом канале и вопреки Федеральному закону № 126–ФЗ от 25.06.2003 «О связи», должной инструкции, уведомлению об ответственности за разглашение информации ограниченной или запрещенной к разглашению в соответствии с Трудовым кодексом Российской Федерации, Кодексом об административных правонарушения, Уголовным кодексом Российской Федерации, а также об имущественной ответственности перед работодателем за причиненный ущерб, связанный с разглашением информации ограниченного доступа, совершил деяние посредством копирования информации с таблицы Exel, а именно телефонных контактов абонентов, их личных сведений, на накопитель информации, а именно на флэш-карту USB, и передал ее неизвестному лицу, не являющемуся сотрудником данной организации. В соответствии с установленными данными суд приговорил подсудимого Б. по ч.3 ст. 272 УК РФ[2].

Приговор Автозаводского районного суда города Тольятти Самарской области вынесен в отношении Д. по ч.3 ст. 272 УК РФ. Судом установлено,

---

[1] См. Приговор Ленинского районного суда города Севастополь № 1-362/2023 от 18 сентября 2023 года по делу № 1-362/2023. [Электронный ресурс]. URL: https://sudact.ru/regular/doc/B47GXnZWo1WN/ (дата обращения: 27.03.2024).

[2] См. Приговор Октябрьского районного суда г. Ростов-на-Дону № 1-470/2023 от 15 сентября 2023 года по делу № 1-470/2023. [Электронный ресурс]. URL: https://sudact.ru/regular/doc/RrV7B2BPCtZX/ (дата обращения: 27.03.2024).

что гражданин Д. умышленными действиями совершил неправомерный доступ к охраняемой законом компьютерной информации без согласия владельца, а именно гражданин Д., не принимая во внимание требования должностной инструкции, с которой был ознакомлен в должном порядке, положения Федерального закона «О персональных данных», а также иных нормативных правовых актов, раскрыл сведения, составляющие коммерческую тайну, а именно: воспользовавшись своим должностным положением и доступом к коммерческой информации, передал посредством сети «Telegram» неустановленному лицу информацию, содержащую абонентские номера, лицевые карточки абонентов, а также доступ к учетным записям в виде логинов и паролей. Данные действия стали систематическими, так как у гражданина Д. изначально возник преступный умысел, направленный на незаконное разглашение сведений, составляющих коммерческую тайну, с использованием своего служебного положения, из корыстной заинтересованности он незаконно копировал компьютерную информацию. В связи с этим судом вынесено следующее решение: признать виновным гражданина Д. в совершении преступления, предусмотренного ч.3 ст. 272 УК РФ, и назначить ему наказание в виде лишения свободы на срок 10 месяцев[1].

Комсомольским районным судом г. Тольятти Самарской области 23 июля 2021 года установлено, что Гражданин Б. не принимая во внимание требования должностной инструкции, с которой был ознакомлен в должном порядке, положения Федерального закона «О персональных данных», а также Федерального закона № 126-ФЗ от 07.07.2003 «О связи» раскрыл сведения, составляющие коммерческую тайну. Как сотрудник ПАО «В..», был наделен полномочиями по обработке персональных данных физических лиц –

[1] См. Приговор Автозаводского районного суда г. Тольятти Самарской области № 1-656/2021 от 26 июля 2021 года по делу № 1-656/2021. [Электронный ресурс]. URL: https://sudact.ru/regular/doc/ZazqFf6KGXoQ/ (дата обращения: 27.03.2024).

абонентов ПАО «В..», в том числе по сбору, хранению, вводу, использованию, изменению и уничтожению обрабатываемых персональных данных, а также по оказанию клиентам компании абонентских услуг, в том числе услуги предоставления детализации. Но, преследуя корыстную цель, а именно получение незаконного дополнительного заработка, и осознавая противоправность своих действий, передал неустановленному лицу посредством переписки в сети «Telegram» детализацию телефонных соединений, номера телефонов абонентов. На основании изложенного судом вынесено следующее решение: признать гражданина Б. виновным в совершении преступления, предусмотренного ч.3 ст. 272 УК РФ и назначить ему наказание в виде штрафа 10000 рублей, с лишением права занимать должности специалистов разных категорий по продаже товаров и услуг[1].

Согласно диспозиции статей 273 УК РФ и 379 УК Туркменистана (созданием, использованием и распространением вредоносных компьютерных программ) субъективную сторону деяния следует определять только прямым умыслом. Иными словами, сам процесс создания, использования, распространения вредоносных программ является совокупностью сложных действий, направленных на создание вредоносной программы, а далее ее распространением, что по своей сути не может определяться неосторожностью. Преступник имеет все возможности оценить общественно опасные последствия, а также морально-психологически оценивает свои действия как фактор агрессивного влияния на информационные процессы. Особенность субъективной стороны данного деяния в том, что исполнителем является лицо, имеющее навыки программирования.

По мнению А.Н. Попова, «состав преступления характеризуется прямым умыслом. Виновный осознает, что создает, использует или

[1] См. Приговор Комсомольского районного суда г. Тольятти Самарской области № 1-242/2021 от 23 июля 2021 года по делу № 1-242/2021. [Электронный ресурс]. URL: https://sudact.ru/regular/doc/7GwYuFr5wOog/ (дата обращения: 27.03.2024).

распространяет вредоносные программу или файл, заведомо для него приводящие к несанкционированным действиям, и желает этого»[1].

А.Г. Волеводз исходит из аналогичной позиции, что субъективная сторона данного преступления всегда выражена в форме прямого умысла[2].

По мнению Л.В. Иногамовой-Хегай, А.И. Рарога, А.И. Чучаева субъективная сторона данного деяния всегда характеризуется осознанным подходом к совершаемому противоправному акту. Само преступленное действие (создание, использование и распространение вредоносных программ) – предполагает намеренный мыслительный процесс, обусловленный совершением информационного противоправного акта, с вытекающими тяжкими последствиями[3].

Согласно п. 15 Постановления Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть “Интернет”», под тяжкими последствиями как квалифицирующим признаком в статьях 272 - 274.1 УК РФ следует понимать, в частности, длительную приостановку или нарушение работы предприятия, учреждения или организации, получение доступа к информации, составляющей охраняемую законом тайну, предоставление к ней доступа неограниченному кругу лиц, причинение по неосторожности смерти, тяжкого вреда здоровью хотя бы одного человека и т.п[4].

---

[1] Попов, А. Н. Преступления в сфере компьютерной информации: учебное пособие / А. Н. Попов. — Санкт-Петербург: Санкт-Петербургский юридический институт (филиал) Университета прокуратуры Российской Федерации, 2018. С. 41.

[2] Волеводз А.Г. Российское законодательство об уголовной ответственности за преступления в сфере компьютерной информации / А.Г. Волеводз // Российский судья. 2002. № 9. С. 42.

[3] См.: Уголовное право. Особенная часть: Учебник. Издание второе исправленное и дополненное / Под ред. доктора юридических наук, профессора Л.В. Иногамовой-Хегай, доктора юридических наук, профессора А.И. Рарога, доктора юридических наук, профессора А.И. Чучаева. — М.: Юридическая фирма «КОНТРАКТ»: ИНФРАМ, 2008. — 800 с.

[4] См.: Постановление Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных

Примеры существуют и в отечественной судебной практике. Коминтерновский районный суд г. Воронежа рассматривал преступление, предусмотренное ч. 3 ст. 273 УК РФ. Исходя из материалов дела, гражданин Б. совершил противоправные действия путем распространения вредоносных программ с целью уничтожения компьютерной информации. Преступление было совершенно организованной группой из корыстной заинтересованности. Обстоятельства преступления, представленные в суд, указывают, что гражданин Б. по приглашению знакомого вступил в организованную преступную группу, которая была создана с целью вмешательства в программную систему ОАО «ВОР.» с использование вредоносного программного обеспечения для осуществления постоянного недолива топлива при заправке автотранспорта. Дело в отношении гражданина Б. было выделено в отдельное производство. Также установлено, что в действиях лиц содержался прямой умысел, и эти лица имели корыстную заинтересованность – извлечение прибыли путем продажи нереализованного нефтепродукта. Действия группы лиц привели к тяжким последствиям. Исходя из совокупности всех обстоятельств дела гражданин Б. был признан виновным и судом назначено наказание в виде лишения свободы на 1 год и 6 месяцев[1].

Приговор Мещанского районного суда г. Москвы. Судом было уставлено, что гражданин Ф. создал, распространил вредоносную программу с целью несанкционированного вмешательства и уничтожения компьютерной информации из корыстной заинтересованности. Гражданин Ф., имея умысел, а также необходимые технические познания, создал вредоносную программу для применения в системе Windows с целью обхода согласования

преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включаясеть «Интернет» // СПС«КонсультантПлюс». [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_434573/ (дата обращения: 26.10.2023).

[1] См.: Приговор Коминтерновского районного суда г. Воронеж от 24 апреля 2017 года по делу № 1-271/2017. [Электронный ресурс]. URL: dvocate-service.ru/sud-praktika/ugolovnye-dela/prigovory-sudov-po-st.-273-uk-rf-sozdanie-ispolzovanie-i-rasprostranenie-vredonosnyh-kompjuternyh-programm/prigovor-suda-po-ch.-3-st.-273-uk-rf--1-2712017--sozdanie-ispolzovanie-i-rasprostranenie-vredonosnyh-kompjuternyh-programm.html (дата обращения: 27.03.2024).

администратора на вход в информационную систему компании и внедрения в систему связанных компьютерных устройств для удаления компьютерной информации. Гражданин Ф. вину полностью признал, с обвинением согласился. Судом было принято решение о назначении наказания по ч. 3 ст. 273 УК РФ в виде лишения свободы на 1 год[1].

В то же время при анализе уголовного кодекса Туркменистана возникает определенная неясность в понимании, какие именно последствия следует квалифицировать как тяжкие в контексте статьи 379 УК Туркменистана. В этом плане предлагаем определить перечень тяжких последствий. Под тяжкими последствиями (квалифицирующий признак) в статьях 373-379 УК Туркменистана следует понимать длительную приостановку функционирования национальной электронной системы, информационной системы критически важных государственных предприятий, иных предприятий любой формы собственности, правовая защита которых установлена действующим законодательством Туркменистана.

Кроме того, рассматривая вопросы квалификации действий в рамках ст. 273 УК РФ и 379 УК Туркменистана следует обратить внимание, что прямой умысел характеризуется когортой специфических фактологических аспектов[2].

Учитывая высокий уровень профессионализма лиц, которые могут совершать такого рода преступления, а также их способность к предвидению последствий своих действий, предположение о том, что они действуют с прямым умыслом, представляется вполне оправданным.

Помимо указанных двух статей в разряд сходных можно отнести еще два состава преступления: ст. 274 УК РФ (нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и

---

[1] См.: Приговор Мещанского районного суда г. Москвы от 19 мая 2017 года. [Электронный ресурс]. URL: https://mos-gorsud.ru/rs/meshchanskij/ (дата обращения: 27.03.2024).

[2] Постановление Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» //СПС«КонсультантПлюс». [Электронный ресурс]. URL:https://www.consultant.ru/document/cons_doc_LAW_43457

информационно-телекоммуникационных сетей) и ст. 376 УК Туркменистана (Нарушение нормальной работы информационной системы и информационно-телекоммуникационной сети)[1].

Р.Р. Гайфутдинов *отмечает, «Уголовная ответственность может наступать только при неосторожной форме вины (по легкомыслию и небрежности)»*[2]. Иными словами, лицо имеет возможность сознательно относится к последствиям, но при этом халатно относиться к выполнению своих обязанностей[3].

Вместе с тем руководствуясь ст. 274 УК РФ и 376 УК Туркменистана лицо, совершая действия, предусмотренные ч.1 данных статей, зачастую не осознает наступления более тяжких последствий, предусмотренных квалифицирующими признаки. Исходя из этого при квалификации преступления, следует иметь ввиду, что основной состав преступления мог совершаться с прямым умыслом, однако в случае расширения уровня общественно опасных последствий лицо возможно не имело возможности предвидеть итог своим действий.

Некоторые ученые придерживаются точки зрения, согласно которой субъективная сторона данных деяний характеризуется виной в форме умысла: «Субъективная сторона создания, использования и распространения компьютерных программ или информации, заведомо предназначенных для совершения атак на объекты критической информационной инфраструктуры, характеризуется прямым умыслом. Лицо, совершая те или иные действия, должно осознавать, что они направлены на публичные

---

[1] Уголовный Кодекс Туркменистана от 12 июня 1997 № 222-I. [Электронный ресурс]. URL: online.zakon.kz/Document/? Doc_id=3129586 (дата обращения: 21.08.2024); Уголовный Кодекс РФ от 13 июня 1996 № 63-ФЗ // Собрание законодательства РФ. – 1996. – № 25.

[2] Гайфутдинов Р. Р. Понятие и квалификация преступлений против безопасности компьютерной информации: диссертация ... кандидата Юридических наук: 12.00.08 / Гайфутдинов Рамиль Рустамович; [Место защиты: ФГАОУ ВО «Казанский (Приволжский) федеральный университет»]. 2017. С. 22.

[3] См.: там же.

информационные ресурсы, обладающие исключительной важностью для общества и государства и включённые в соответствующий реестр»[1].

Кроме того, следует отметить, что вопросы отнесения мотивов и целей, которыми руководствуется преступник, не имеют основания быть признанными обязательными при квалификации преступлений такого характера. По мнению А.Л. Пелевиной, «такие обстоятельства как мотивы и цели преступлений в сфере компьютерной информации следует учитывать при назначении наказания»[2]. Факт применения технического средства, вредоносной программы, либо совершения иных манипуляций в информационном пространстве, а также по отношению к компьютерной информации, является основанием квалификации таких действий. При этом квалифицируя действия следует учитывать не только вид манипуляции, но средства совершения преступного акта.

На основании вышеизложенного следует выделить несколько видов субъекта преступлений в сфере компьютерной информации по уголовному законодательству Российской Федерации и Туркменистана: общий субъект (16 лет; субъекты с факультативные признаки (служебное положение и специальные технические познания[3])[4]. Субъективная сторона отдельных видов преступлений в сфере компьютерной информации по уголовному законодательству Российской Федерации и Туркменистана выражается в форме прямого умысла, но также имеются обстоятельства, подтверждающие позицию, что ряд деяний может совершаться по неосторожности.

---

[1] Русскевич Е.А. Уголовное право и «цифровая преступность»: проблемы и решения: монография. 2-е изд., перераб. и доп. – М.: ИНФРА-М, 2022. С. 242.

[2] Пелевина, А.В. Общая характеристика преступлений в сфере компьютерной информации. Пробелы в российском законодательстве, 2015. С. 211.

[3] См.: Корпеев, А.Г. О субъекте преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (технологий), по уголовному законодательству Российской Федерации и Туркменистана / А. Г. Корпеев // Вопросы российского и международного права. – 2024. – Т. 14, № 1-1. С. 569-578.

[4] Данную позицию поддержали 56,3 % опрошенных респондентов.

Глава 3. Соотношение квалифицирующих и особо квалифицирующих признаков преступлений в сфере компьютерной информации по современному уголовному законодательству России и Туркменистана

3.1. Соотношение квалифицирующих признаков преступлений в сфере компьютерной информации по современному уголовному законодательству России и Туркменистана[1]

По мнению М.А. Авдеева и А.С. Штранца квалифицирующие признаки относятся к категории отягчающих обстоятельств, установленных общей частью уголовного законодательства[2].

Довольно интересной, на наш взгляд, выглядит группа delictum в сфере компьютерной информации. Эти преступления характеризуются уникальными конструктивными особенностями, которые находят своё отражение в квалифицирующих признаках, что делает их особенно интересными для изучения.

В рамках уголовного законодательства каждое конкретное преступление характеризуется определенным набором элементов, которые в совокупности формируют его основную структуру. Этот комплекс включает в себя три ключевых компонента: гипотезу, диспозицию и санкцию. Однако, помимо этих базовых элементов, законодательство предусматривает и дополнительные, более специфические компоненты, которые могут усиливать ответственность за совершенное деяние. Квалифицирующие признаки, играют важную роль в оценке степени общественной опасности деяния. Они

---

[1] Корпеев, А.Г. О квалифицирующих признаках преступлений в сфере компьютерной информации по уголовному законодательству России и Туркменистана // Вестник ТГУПБП. 2024. №1. С. 29-36

[2] Авдеев, М.А., Штранц, А.С. Общая характеристика квалифицирующих признаков и их значение при конструировании составов преступлений // Актуальные проблемы государства и права. 2019. Т. 3. № 9. С. 68.

служат для подчеркивания того, что в определённых условиях данное преступное деяние может представлять собой значительную угрозу для общественного порядка и безопасности.

В системе уголовного законодательства Российской Федерации и Туркменистана существуют общие конструкционные особенности в части квалифицирующих признаков.

В уголовном законодательстве двух стран имеется унифицированный по форме содержания квалифицирующий признак «использование информационно-телекоммуникационных сетей, в том числе сети “Интернет”». Вместе с тем на сегодняшний день у правоприменителей (судов) имеются существенные трудности в вопросах квалификации таких деяний.

По мнению Н.В. Летелкина, «большинство составов «Особенной части» УК РФ де-юре лишены квалифицирующего признака «с использованием информационно-телекоммуникационных сетей», но фактически совершаются с использованием данных сетей, например, использование данных сетей активно применяется при деяниях, направленных на незаконный оборот оружия, боеприпасов, взрывных устройств»[1]. *Несмотря на наличие квалифицирующих составов с вышеупомянутом квалифицирующим признаком, судами также нередко данные преступления квалифицируются неверно, вопреки тому, что факт использования информационно-телекоммуникационных сетей является бесспорно подтверждённым*[2].

В Республике Коми вынесено решение по ч. 1 ст. 282 УК РФ в отношении Б. Суд установил, что гражданин Б., используя различные имена (псевдонимы) публиковал, используя информационно-телекоммуникационные сети, на сайте местной газеты сведения с целью разжигания вражды на почве различий национального происхождения, а

---

[1] Летелкин, Н.В. Уголовно-правовое противодействие преступление преступлениям, совершаемым с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет»): монография / отв. ред. А.В. Петрянин. – Москва: Проспект, 2021. С. 89.
[2] См. Там же.

также с целью оскорбления чувств верующих. Судом также установлено, что при выполнении объективной стороны осужденным использовалась информационно-телекоммуникационная сеть, однако при вынесении наказания факт использования информационно-телекоммуникационной сети не учитывался[1].

Также стоит отметить неверную квалификацию имущественных преступлений, сопряженных с использованием информационно-телекоммуникационных сетей. Согласно материалам Тушинского районного суда Москвы, гражданин А., располагая информацией о банковском счете гражданина Л.А., используя компьютерное устройство с выходом в сеть «Интернет» перевел с расчетного счета гражданина Л.А. денежные средства, на ранее открытый собственный счет, тем самым совершив тайное хищение денежных средств, что нанесло ущерб гражданину Л.А. в размере 6000 рублей. Данное деяние было квалифицированно по п. ч. 1 т. 158 УК РФ (кража), хотя факт использования информационно-телекоммуникационных сетей был признан как материалами дела, так и судом в рамках судебного разбирательства[2].

Также следует выделить такой квалифицирующий признак, как наступление тяжких последствий. В составах преступлений в сфере компьютерной информации в УК РФ и УК Туркменистана такой квалифицирующий признак присутствует, например, в п.4 ст. 272 УК РФ, в ч.3. ст. 374 УК Туркменистана[3]. Под данным квалифицирующим признаком понимается в первую очередь - неправомерное воздействие на критическую информационную инфраструктуру предприятия, организации, а также причинение вреда здоровью. В УК Туркменистана под критической

---

[1] Интернет-пользователь осужден за «эмоциональные» письма в СМИ с домашнего компьютера // Право.ru. [Электронный ресурс]. URL. https://pravo.ru/news/view/59120/ (дата обращения: 12.03.2024).

[2] Приговор Тушинского районного суда Москвы от 26.06.2020 № № 1-420/20. [Электронный ресурс]. URL: https://www.mos-gorsud.ru/rs/tushinskij/cases/docs/content/b69a423b-520c-43ba-91ad-1f0dedbc7c86 (дата обращения: 12.03.2024).

[3] См.: Корпеев, А.Г. О квалифицирующих признаках преступлений в сфере компьютерной информации по уголовному законодательству России и Туркменистана // Вестник ТГУПБП. 2024. №1. С. 29-36

информационной инфраструктурой понимается национальная информационная система, данные понятия являются идентичными. При этом под национальной информационной инфраструктурой понимается совокупность всех информационных систем, обеспечивающих работу государственных органов федерального и регионального уровня в сфере образования, промышленности, здравоохранения государственной безопасности, предприятий оборонно-промышленного комплекса.

В качестве квалифицирующего признака в составах компьютерных преступлений в Российской Федерации выделяется крупный ущерб (ч.2. ст. 272). Крупный ущерб выражается в материально-денежном эквиваленте, стандартное понимание крупного ущерба — это сумма выше одного миллиона рублей[1].

Так, Чкаловским районным судом рассматривалось дело № 1-609/2017, в рамках которого Ж., осознавая, что у него отсутствует заключенный договор с корпорацией, в том числе предусматривающий обработку компьютерной информации, модифицировал сведения и скопировал на электронный носитель с целью дальнейшей реализацией. Данное преступное деяние привело к нанесению крупного ущерба корпорации в размере 3,5 миллионов рублей. Действия лица были квалифицированы по ч.2. ст. 272 УК РФ[2].

В ч. 2 ст. 272 УК РФ также предусмотрен такой квалифицирующий признак как корыстная заинтересованность. Корыстная заинтересованность – это мотивация преступного поведения, сопряженная со стремлением виновного к получению выгоды имущественного характера[3]. Так, Пленум

---

[1] Уголовный Кодекс РФ от 13 июня 1996 № 63-ФЗ. [Электронный ресурс]. URL.: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения 22.05.2024).

[2] Приговор Чкаловского районного суда города Екатеренбург от 07.06.2017 по делу № 1-609/2017. [Электронный ресурс]. URL: https://sud-praktika.cloud/precedent/420329.html (дата обращения: 14.02.2025).

[3] См.: Корпеев, А.Г. О квалифицирующих признаках преступлений в сфере компьютерной информации по уголовному законодательству России и Туркменистана // Вестник ТГУПБП. 2024. №1. С. 29-36; Постановление Пленума Верховного Суда РФ от 16.10.2009 № 19 «О судебной практике по делам о злоупотреблении должностными полномочиями и о превышении должностных полномочий» // СПС «КонсультантПлюс». [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_93013/ (дата обращения: 15.11.2023).

Верховного Суда Российской Федерации в п. 16 постановления от 16 октября 2009 г. № 19 разъясняет, что корыстная заинтересованность – стремление путем совершения неправомерных действий получить для себя или других лиц выгоду[1] имущественного характера[2]. Корыстная заинтересованность является одним из маркеров совершения компьютерных преступлений: зачастую лица ради получения определенного денежного или иного имущественного дохода, а также иных материальных благ, являясь при этом должностными лицами, осуществляют противоправные действия, связанные с копированием либо модификацией компьютерной информации.

Советский районный суд г. Самара рассматривал уголовное дело в отношении Ф., который совершил из корыстной заинтересованности несколько противоправных доступов к компьютерной информации с ограниченным доступом. Согласно материалам дела, Ф., используя свое служебное положение, имел доступ к списку абонентов корпорации, в которой он работал. Завладев этими данными, он, пользуясь специальным интернет-сервисом, выяснял о наличии на лицевом счете абонента денежных средств. При получении такой информации без соответствующего заявления владельца абонентского номера, используя специальную программу, Ф. модифицировал данные и получал доступ к лицевому счету абонента, а денежные средства (корыстная заинтересованность), содержащиеся на лицевом счете, переводил на свои банковские карты. Действия лица были квалифицированы по ч.2 и ч. 3 ст. 272 УК РФ[3].

В качестве квалифицирующих признаков при совершении преступлений в сфере компьютерной информации выделяются и такие признаки, как

---

[1] См.: Корпеев, А.Г. О квалифицирующих признаках преступлений в сфере компьютерной информации по уголовному законодательству России и Туркменистана // Вестник ТГУПБП. 2024. №1. С. 29-36

[2] Постановление Пленума Верховного Суда РФ от 16.10.2009 № 19 «О судебной практике по делам о злоупотреблении должностными полномочиями и о превышении должностных полномочий» // СПС «КонсультантПлюс». [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_93013/ (дата обращения: 15.11.2023).

[3] Приговор Советского районного суда города Самара от 13.02.2017 по делу № 1-61/2017. [Электронный ресурс]. URL: https://sud-praktika.cloud/precedent/203577.html (дата обращения 14.02.2025).

«совершенное группой лиц по предварительному сговору» или «совершенное организованной группой лиц» (ч. 3 ст. 272 УК РФ, ч. 2 ст. 273 УК РФ, ч. 4 ст. 274 [1]УК РФ)[1]. Согласно ст. 35 УК РФ *преступление признается совершенным группой лиц по предварительному сговору, когда в деянии приняло участие несколько лиц, имевших заранее конкретные договоренности*[2]*. В свою очередь, под организованной группой понимается объединение лиц с устойчивой формой организации для осуществления нескольких противоправных действий*[3].

Конечно, компьютерные преступления не являются исключением из когорты преступлений, которые могут совершать вышеуказанным организованным способом. Примером того являются различные объединения хакерских групп.

Согласно материалам дела Перовского районного суда города Москвы У.С. совершил неправомерный доступ к компьютерной информации в составе организованной группы. У.С., обладая техническим познаниями в сфере программного обеспечения, согласился на реализацию преступного плана А.Б., который, в свою очередь, создал организованную группу с целью искажения отчётности кассовых аппаратов и минимизации налогообложения. Действия лиц были квалифицированы по ч.3 ст. 272 УК РФ[4].

В свою очередь, в УК Туркменистана квалифицирующие признаки преступлений в сфере компьютерной информации имеют ряд отличительных особенностей в части своеобразия конструирования и формулирования таких признаков. В этом случае данные квалифицирующие признаки отражают видение законодателем Туркменистана основной проблематики в части

---

[1] Корпеев, А.Г. О квалифицирующих признаках преступлений в сфере компьютерной информации по уголовному законодательству России и Туркменистана // Вестник ТГУПБП. 2024. №1. С. 29-36

[2] Уголовный Кодекс РФ от 13 июня 1996 № 63-ФЗ. [Электронный ресурс]. URL.: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения 22.05.2024).

[3] Уголовный Кодекс РФ от 13 июня 1996 № 63-ФЗ. [Электронный ресурс]. URL.: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения 22.05.2024).

[4] Приговор Перовского районного суда от 10.10.2016 по делу № 1-975/2016. [Электронный ресурс]. URL: https://sud-praktika.cloud/precedent/84286.html (дата обращения: 14.02.2025).

рисков действий, которые могут повлечь повышение общественной опасности некоторых составов преступлений в сфере компьютерной информации[1].

Согласно ч. 2 и 3 ст. 373 УК Туркменистана, ч.2, 3 ст. 374 УК Туркменистана, ч.2, 3 ст. 376 УК Туркменистана в качестве квалифицирующего признака закреплено совершение деяния основного состава преступления в отношении национальной электронной информации и национальной информационной системы, объектов информационно-коммуникационной инфраструктуры[2]. В данном квалифицирующем признаке ключевым словом является «*национальное*», т.е. государственное и все, что связано с государственными структурами, образующими национальную информационную сеть. Национальная электронная информация – это огромная база данных, в которой содержатся различные данные государственной важности, доступные государственным органам и гражданам Туркменистана, имеющим доступ к такой информации. В перечень таких данных можно включить любые сообщения и сведения, передающиеся между государственными органами Туркменистана, хранящиеся в государственных органах, обработка и хранение которых определяется действующим законодательством Туркменистана в сфере применения обработки информации с ограниченным доступом[3].

Национальная информационная система — это разветвлённая система информационных устройств и ресурсов, способствующих обработке информации в рамках государственного образования. В национальную информационную систему входят государственная информационная система, региональная информационная система и система районных образований.

---

[1] Корпеев, А.Г. О квалифицирующих признаках преступлений в сфере компьютерной информации по уголовному законодательству России и Туркменистана // Вестник ТГУПБП. 2024. №1. С. 29-36

[2] Уголовный кодекс Туркменистана от 12.06.1997 № 222-I в ред. от 29.09.2023. Газета Нейтральный Туркменистан. [Электронный ресурс]. URL: https://metbugat.gov.tm/newspaper?id=8291 (дата обращения: 27.10.2023).

[3] См.: Корпеев, А.Г. О квалифицирующих признаках преступлений в сфере компьютерной информации по уголовному законодательству России и Туркменистана // Вестник ТГУПБП. 2024. №1. С. 29-36

С точки зрения безопасности защита национальной информационной системы является приоритетным сегментом уголовно-правовой политики Туркменистана. Данный квалифицирующих признак, по нашему мнению, является смысловой производной преступлений, предусмотренных ст. 274[1] - 274[2] УК РФ. Отличительной особенностью является тот факт, что в УК Туркменистана действия, совершаемые в отношении национальной электронной информации, национальной информационной системы и информационно-коммуникационной инфраструктуры, закреплены в качестве квалифицирующего признака ко многим составам преступлений в сфере компьютерной информации, тогда как в УК РФ предусмотрены отдельные составы преступлений[1].

Еще одним квалифицирующим признаком является повторное совершение одного и того же деяния, предусмотренное ч.2 ст. 374 УК Туркменистана «Принуждение к передаче информации». В данном случае следовало бы провести аналогию с рецидивом (ст. 18 УК Туркменистана), так как первоначально возникает именно такое сравнение. Но при соотношении признаков рецидива и данного вышеуказанного квалифицирующего признака, следует обратить внимание, что рецидивом признается умышленное преступление, совершенное лицом, имеющим судимость за ранее совершенное умышленное преступление[2], однако по смыслу ч.2 ст. 374 УК Туркменистана непонятны критерии привлечения лица к повторной ответственности, а также отсутствуют отсылки к ст. 18 УК Туркменистана. Возникает также вопрос по п. 8 ст. 6 УК Туркменистана, в котором обозначается, что «лицо не может быть подвергнуто повторному осуждению

---

[1] См.: Корпеев, А.Г. О квалифицирующих признаках преступлений в сфере компьютерной информации по уголовному законодательству России и Туркменистана // Вестник ТГУПБП. 2024. №1. С. 29-36

[2] Уголовный кодекс Туркменистана от 12.06.1997 № 222-I в ред. от 29.09.2023. Газета Нейтральный Туркменистан. [Электронный ресурс]. URL: https://metbugat.gov.tm/newspaper?id=8291 (дата обращения: 27.10.2023).

за одно и тоже преступление»[1]. *Если углубиться в семантику, то слово «рецидив» с латинского языка переводится как «возвращающийся», в русском языке слово «рецидив» понимается как повторное явление*[2]. Исходя из вышесказанного, считаем, что квалифицирующий признак «совершение преступления повторно», предусмотренный ч. 2 ст. 374 УК Туркменистана, по уголовно-правовому смыслу и есть рецидив, однако в таком случае следовало бы уточнить формулировку квалифицирующего признака или обозначить отсылку для определения правового смысла применения данного квалифицирующего признака[3].

Вышесказанное подтверждает, что перечень квалифицирующих признаков преступлений в сфере компьютерной информации, предусмотренных уголовным законодательством Российской Федерации и Туркменистана, достаточно широк и разнообразен. Определяются общие подходы к конструированию квалифицирующих признаков таких преступлений, но также имеются и характерные для двух законодательств квалифицирующие признаки. Вместе с тем имеются и семантические особенности некоторых квалифицирующих признаков, требующих уточнение, для справедливого применения таких признаков в правоприменительной практике.

3.2. Соотношение особо квалифицирующих признаков преступлений в сфере компьютерной информации по современному уголовному законодательству России и Туркменистана[4]

---

[1] Уголовный кодекс Туркменистана от 12.06.1997 № 222-I в ред. от 29.09.2023. Газета Нейтральный Туркменистан. [Электронный ресурс]. URL: https://metbugat.gov.tm/newspaper?id=8291 (дата обращения: 27.10.2023).

[2] Уголовное право России. Части Общая и Особенная: учебник (коллектив авторов; под ред. д.ю.н., проф. А.В. Бриллиантова; 3-е изд., перераб. и доп.). – «Проспект», 2021 г. - 1344 с.

[3] Корпеев, А.Г. О квалифицирующих признаках преступлений в сфере компьютерной информации по уголовному законодательству России и Туркменистана // Вестник ТГУПБП. 2024. №1. С. 29-36

[4] При написании параграфа использовалась работа, опубликованная в рамках диссертационного исследования: См. далее по тексту: Корпеев, А.Г. О квалифицирующих признаках преступлений в сфере

В контексте рассматриваемых преступлений в сфере компьютерной информации роль особо квалифицирующих признаков возрастает в связи с уровнем общественной опасности данных деяний под призмой многообразия форм ущерба, который можно нанести противоправным использованием компьютерных устройств для достижения корыстных целей.

Ущерб от преступлений в сфере компьютерной информации может являться колоссальным не только для личности, но и для целого государства. В этом плане ущерб следует разделить исходя из его территориального охвата. Причинение ущерба может сопровождаться уничтожением, блокированием, изменением информации. Ущерб может быть нанесен отдельной личности, ущерб может быть нанесен предприятию либо организации в рамках субъекта либо территориальной единицы, стране, обществу в рамках территориальных границ страны, промышленным предприятиям, обладающим критической инфраструктурой, государственным органам.

Согласно п. 14 постановления Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37 под тяжкими последствиями как квалифицирующим признаком в статьях 272-274[1] УК РФ следует понимать приостановку либо нарушение целостности работы информационной системы различных предприятий и учреждений на длительный период времени, приведшее к незаконному доступу к охраняемой законом информации (в том числе сведениям, составляющим государственную тайну), а также к наступлению последствий в виде тяжкого вреда здоровью[1].

«*Однако благодаря квалифицирующим признакам общественная опасность в какой-то степени приобретает уточняющие грани особо*

компьютерной информации по уголовному законодательству России и Туркменистана // Вестник ТГУПБП. 2024. №1. С. 29-36

[1] Постановление Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть«Интернет»//СПС«КонсультантПлюс». [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_434573/ (дата обращения: 25.09.2024).

опасных последствий[1]. В связи с этим А.Г. Антонова, Е.А. Зорина и Д.В. Крюкова *вводят такое понятие, как кумулятивная общественная опасность, что подразумевает под собой сосредоточение в одном понятии высокого негативного потенциала»*[2].

Особо квалифицирующие признаки являются наивысшей планкой дифференциации ответственности, так как уровень общественной опасности как раз приближается к кумулятивному. Как было сказано ранее, возможности нанесения ущерба компьютерными устройствами неисчерпаемы. «*Важно понимать, что кумулятивность также заключается в том, что данные преступления, предусмотренные главой 28 УК РФ и главой 33 УК Туркменистана, зачастую являются следствием совершения действий, которые квалифицируются иными составами преступлений уголовного закона. Посягательства происходят на одни общественные отношения, но потенциально это влечет последствия для других общественных отношений, охраняемые уголовным законом. Например, неправомерный доступ к компьютерной информации с целью ее копирования может повлечь за собой нарушение авторских прав, мошенничество»*[3].

Комплекс закрепленных в Уголовных кодексах Российской Федерации и Туркменистана особо квалифицирующих признаков преступлений в сфере компьютерной информации говорит лишь о важности данной сферы в рамках уголовно-правовой политики двух стран. В совокупности структура построения и виды таких особо квалифицирующих признаков в уголовном законодательстве двух стран являются идентичными. Основаниями дифференциации уголовной ответственности преступлений в сфере компьютерной информации в рамках уголовных кодексов двух стран является совершение преступления группой лиц по предварительному сговору или

---

[1] Антонов, А.Г., Зорина, Е.А., Крюков, Д.В. К вопросу об общественной опасности неправомерного доступа к компьютерной информации // Вестник Томского государственного университета. Право. 2022. № 44. С.14.
[2] Там же. С. 14.
[3] Антонов, А.Г., Зорина, Е.А., Крюков, Д.В. К вопросу об общественной опасности неправомерного доступа к компьютерной информации // Вестник Томского государственного университета. Право. 2022. № 44. С.14.

организованной группой либо лицом с использованием своего служебного положения, наступление тяжких последствий, причинение крупного ущерба.

В главе 28 УК РФ и 33 УК Туркменистана особо квалифицирующий состав преступлений в сфере компьютерной информации имеет место при наличии одного из нижеследующих особо квалифицирующих признаков: 1) совершение преступления группой лиц по предварительному сговору (п.3 ст. 272 УК РФ, п.2 ст. 273 УК РФ, ч. 4 ст. 274[1] УК РФ, п.3 ст. 373 УК Туркменистана, п.3 ст. 375 УК Туркменистана, п.3 ст. 379 УК Туркменистана, п.3 ст. 380 УК Туркменистана)[1], 2) совершение преступления организованной группой (п.3. ст. 272 УК РФ, п.2 ст. 273 УК РФ, ч.4 ст. 274[1] УК РФ, п.3 ст. 373 УК Туркменистана, п.3 ст. 374 УК Туркменистана, п.3 ст. 375 УК Туркменистана, п. 3 ст. 376 УК Туркменистана, п.3 ст. 379 УК Туркменистана, п.3 ст. 380 УК Туркменистана, п.3 ст. 382 УК Туркменистана)[2], 3) тяжкие последствий (п.4 ст. 272 УК РФ, п.3 ст. 272 УК РФ, ч.2 ст. 274 УК РФ, п.3 ст. 374 УК Туркменистана, п. 3 ст. 376 УК Туркменистана, п.3 ст. 379 УК Туркменистана, п.3 ст. 380 УК Туркменистана)[3], 4) совершение преступления при проведении массовых мероприятий (п.4 ст. 378 УК Туркменистана)[4], 5) совершение преступления преступным сообществом (п.3 ст. 374 УК

---

[1] Уголовный кодекс Туркменистана от 12 июня 1997 № 222-I. [Электронный ресурс]. URL: online.zakon.kz/Document/? Doc_id=3129586 (дата обращения: 07.10.2024); Уголовный Кодекс РФ от 13 июня 1996 № 63-ФЗ. [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения 15.01.2024).

[2] Уголовный кодекс Туркменистана от 12 июня 1997 № 222-I. [Электронный ресурс]. URL: online.zakon.kz/Document/? Doc_id=3129586 (дата обращения: 07.10.2024); Уголовный Кодекс РФ от 13 июня 1996 № 63-ФЗ. [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения 15.01.2024).

[3] Уголовный кодекс Туркменистана от 12 июня 1997 № 222-I. [Электронный ресурс]. URL: online.zakon.kz/Document/? Doc_id=3129586 (дата обращения: 07.10.2024); Уголовный Кодекс РФ от 13 июня 1996 № 63-ФЗ. [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения 15.01.2024).

[4] Уголовный кодекс Туркменистана от 12 июня 1997 № 222-I. [Электронный ресурс]. URL: online.zakon.kz/Document/? Doc_id=3129586 (дата обращения: 07.10.2024); Уголовный Кодекс РФ от 13 июня 1996 № 63-ФЗ. [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения 15.01.2024).

Туркменистана), 6) совершение преступления в условиях режима чрезвычайного или военного положения (п. 4 ст. 378 УК Туркменистана)[1].

Согласно ч. 2 ст. 35 УК РФ преступление признается совершенным группой лиц по предварительному сговору, если в нем участвовали лица, заранее договорившиеся о совместном совершении преступления, согласно ч.1 ст. 31 УК Туркменистана - если в нём участвовали два и более лица, заранее договорившиеся о совместном совершении преступления[2]. Содержание диспозиции в двух кодексах является идентичным, за исключением акцента законодателя Туркменистана на количественном аспекте факта признания преступления совершенным группой лиц по предварительному сговору, однако это вытекает из того, что в ст. 31 УК Туркменистана, в отличие от ст. ч.1 ст. 35 УК РФ (преступление признается совершенным группой лиц, если в его совершении совместно участвовали два или более исполнителя без предварительного сговора[3]), отсутствует определение такой формы соучастия, как преступление[4], совершенное группой лиц, соответственно[5], конкретика в отношении количества участников закреплена в диспозиции ч. 1 ст. 31 УК Туркменистана[6].

Ключевым признаком данной формы соучастия является наличие предварительного сговора, который в соответствии с п.10 Постановления Пленума Верховного суда РФ от 27.01.1999 № 1 «предполагает выраженную в любой форме договоренность двух или более лиц, состоявшуюся до начала

---

[1] Уголовный кодекс Туркменистана от 12 июня 1997 № 222-I. [Электронный ресурс]. URL: online.zakon.kz/Document/? Doc_id=3129586 (дата обращения: 07.10.2024); Уголовный Кодекс РФ от 13 июня 1996 № 63-ФЗ. [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения 15.01.2024).

[2] Уголовный кодекс Туркменистана от 12 июня 1997 № 222-I. [Электронный ресурс]. URL: online.zakon.kz/Document/? Doc_id=3129586 (дата обращения: 07.10.2024); Уголовный Кодекс РФ от 13 июня 1996 № 63-ФЗ. [Электронный ресурс]. URL.: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения 23.09.2024) .

[3] Уголовный Кодекс Туркменистана от 12 июня 1997 № 222-I. [Электронный ресурс]. URL: online.zakon.kz/Document/? Doc_id=3129586.

[4] См.: Корпеев, А.Г. О квалифицирующих признаках преступлений в сфере компьютерной информации по уголовному законодательству России и Туркменистана // Вестник ТГУПБП. 2024. №1. С. 29-36

[5] См.: Там же.

[6] Уголовный Кодекс Туркменистана от 12 июня 1997 № 222-I. [Электронный ресурс]. URL: online.zakon.kz/Document/? Doc_id=3129586.

совершения действий, непосредственно направленных на лишение жизни потерпевшего. При этом, наряду с соисполнителями преступления, другие участники преступной группы могут выступать в роли организаторов, подстрекателей или пособников убийства»[1].

Так, согласно материалам Головинского районного суда г. Москва от 25 мая 2023 года по делу № 1-342/2023, К. совершил неправомерный доступ к охраняемой законом компьютерной информации (ч. 3 ст. 272 УК РФ), повлекший копирование компьютерной информации. Преступление было совершено группой лиц по предварительному сговору из корыстной заинтересованности, путем сговора с иными неустановленными лицами, выступающими в данной ситуации в роли подстрекателей, тогда как К. была отведена роль исполнителя. Судом установлено, что К. получил от неустановленного лица заявку на информацию об абонентах ПАО «МТС», в которой имел законный доступ К.[2].

В контексте преступлений в сфере компьютерной информации, по законодательству Российской Федерации и Туркменистана, группа лиц по предварительному сговору — это объединение лиц, имеющих умысел в получении доступа к цифровым сведениям. *«Сговором следует считать согласие всех участников преступления, вне зависимости от вида коммуникации, воля может быть выражена с помощью вербальных методов коммуникации (согласие словами) либо невербальными способами (жестом, мимикой). Обычно контингент объединения таких лиц с целью совершения преступлений преимущественно составляют лица, имеющие полномочия в рамках своего служебного положения на доступ либо обработку конфиденциальной информации, а также третьи лица, не имеющие*

---

[1] См.,: Постановление Пленума Верховного Суда РФ от 27.01.1999 N 1 (ред. от 03.03.2015) «О судебной практике по делам об убийстве (ст. 105 УК РФ)». [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_21893/; Уголовное право. Особенная часть. : учебник / В. В. Бабурин, М. В. Бавсун, И. А. Белецкий [и др.] ; под ред. М. В. Бавсуна. — Москва : КноРус, 2022. — 577 с.

[2] См. Приговор Головинского районного суда г. Москва от 25 мая 2023 года по делу № 1-342/2023. [Электронный ресурс]. URL: https://mos-gorsud.ru/rs/golovinskij/services/cases/criminal/details/9959a360-e5c5-11ed-a575-f7b7b38a87de?caseNumber=1-342/2023 (дата обращения: 30.09.2024).

служебного положения, но выступающие инициаторами незаконного завладения охраняемой законом информации»[1].

Так, П. совершил неправомерный доступ к охраняемой законом компьютерной информации, повлекший модификацию компьютерной информации, с использованием служебного положения, а именно посредством мобильной связи, т.о. он согласился осуществить изменения информации в личной карточке абонента. Действия соучастников привели к наступлению последствий, предусмотренных ст. 272 УК РФ. Суд квалифицировал действия П. по ч.3 ст. 272 УК РФ - деяние, совершенное группой лиц по предварительному сговору. Данный вид преступлений, совершаемых группой лиц по предварительному сговору, предусмотренных ч. 3 ст. 272 УК РФ и ч.3 ст. 375 УК Туркменистана, является весьма распространённым[2].

Особо квалифицирующий признак совершения деяния организованной группой является распространённым признаком, предусмотренным в конструкции составов преступлений в сфере компьютерной информации в УК РФ и в УК Туркменистана. В соответствии с ч.3 ст. 35 УК РФ и ч. 2 ст. 31 УК Туркменистана понятие «совершение преступления организованной группой» является унифицированным и определяется как преступление, совершенное устойчивой группой лиц, заранее объединившихся для совершения одного или нескольких преступлений[3].

В плоскости преступлений в сфере компьютерной информации организованные группы имеют сложную, а также универсальную системно-организационную форму объединения. Определенно действия лиц в рамках

---

[1] См. например: Прокурор разъясняет. Разъяснение понятий совершения преступлений группой лиц, группой лиц по предварительному сговору. [Электронный ресурс]. URL: https://epp.genproc.gov.ru/ru/web/proc_42/activity/legal-education/explain?item=49713816 (дата обращения: 23.04.2025); Уголовное право. Особенная часть. : учебник / В. В. Бабурин, М. В. Бавсун, И. А. Белецкий [и др.] ; под ред. М. В. Бавсуна. — Москва : КноРус, 2022. — 577 с.

[2] Приговор Коптевского районного суда г. Москва от 6.06.2018 № 1-121/18 // URL: https://mos-gorsud.ru/rs/koptevskij (дата обращения: 03.10.2024)

[3] Уголовный кодекс Туркменистана от 12 июня 1997 № 222-I. [Электронный ресурс]. URL: online.zakon.kz/Document/? Doc_id=3129586 (дата обращения: 07.10.2024) Уголовный Кодекс РФ от 13 июня 1996 № 63-ФЗ. [Электронный ресурс]. URL.: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения 22.05.2024).

таких групп выражаются четко спланированным набором действий, направленных на достижения целей группы. К тому же совершение преступлений в сфере компьютерной информации подразумевает также дистанционный метод коммуникации членов группы (онлайн)[1].

Еще одной проблемой, которая укладывается в смысловой контекст данного квалифицирующего признака, является рассеянное нахождение участников организованной группы: участники группы могут находиться в различных точках мира, но при этом централизованно выполнять возложенный на них функционал с помощью различных информационных технологий, предоставляющих возможности воздействия на компьютерную информацию из различных уголков мира.

Также еще одной формой соучастия в преступлениях в сфере компьютерной информации является преступное сообщество. Такая форма соучастия преступлений в сфере компьютерной информации предусмотрена только в УК Туркменистана. Согласно ст. 31 УК Туркменистана под преступным сообществом понимаются лица, предварительно сорганизовавшиеся в устойчивую, сплочённую, управляемую организацию, созданную для совершения тяжких и особо тяжких преступлений[2].

Вышеуказанная форма соучастия в отличие от других форм по своей социально-правовой сущности определяется как сверхопасное структурное объединение. В соответствии с п. 7 Постановления Пленума Верховного Суда РФ от 10.06.2010 № 12 «О судебной практике рассмотрения уголовных дел об организации преступного сообщества (преступной организации) или участии в нем (ней)»: *«Уголовная ответственность за создание преступного*

---

[1] См. например: И.Р. Бегишев, З.И. Хисамова, С.Г. Никитин. Организация хакерского сообщества: криминологический и уголовно-правовой аспекты // Всероссийский криминологический журнал. 2020. Т.14, №1. С.99, 102; F. Varese (ed), What is Organised Crime? vol I . P. 27 – 55. [Электронный ресурс]. URL: https://federicovarese.com/wp-content/uploads/2019/07/varese-2017-redefining-organised-crime-03.pdf (дата обращения: 19.01.2024); Varese, F. Organized Crime: Critical Concepts in Criminology (London , Routledge , 2010) vol I. P. 11 – 33.

[2] Уголовный кодекс Туркменистана от 12 июня 1997 № 222-I. [Электронный ресурс]. URL: online.zakon.kz/Document/? Doc_id=3129586 (дата обращения: 07.10.2024).

сообщества (преступной организации) в целях совместного совершения одного или нескольких тяжких или особо тяжких преступлений наступает с момента фактического образования указанного преступного сообщества (преступной организации), то есть с момента создания в составе организованной группы структурных подразделений или объединения организованных групп и совершения ими действий, свидетельствующих о готовности преступного сообщества (преступной организации) реализовать свои преступные намерения, независимо от того, совершили ли участники такого сообщества (организации) запланированное тяжкое или особо тяжкое преступление»[1].

Концептуально в разрезе рассматриваемых преступлений в сфере компьютерной информации такая особенность в виде требований к участникам преступного объединения является наличием узкоспециализированных знаний в области программирования, информационных технологий.

Если мы говорим о преступлениях в сфере компьютерной информации, то профессионализм в данном случае является основным образующим данное преступное сообщество элементом. Подобные преступные сообщества для совершения преступлений в сфере компьютерной информации создаются из специалистов в сфере информационных технологий.

В повседневной жизни такие сообщества называются хакерскими (хакер в переводе означает «взломщик»[2]). Такие группировки повседневно атакую банки, предприятия, физических лиц как в Туркменистане, так и в Российской Федерации. Одним из таких примеров является недавняя атака хакерского сообщества sudo rm-RF, на российскую ВГТРК, из-за которой нарушилось

---

[1] Постановление Пленума Верховного Суда РФ от 10.06.2010 N 12 «О судебной практике рассмотрения уголовных дел об организации преступного сообщества (преступной организации) или участии в нем (ней)». [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_101362/ (дата обращения: 07.10.2025).

[2] [Электронный ресурс]. URL: https://ht-lab.ru/obuchenie/slovari/kratkiy-slovar-it/khaker/ (дата обращения 20.05.2025).

телерадиовещание на всю Россию. Предположительно, участникам группировки удалось подкупить сотрудника ВГТРК с целью завладения доступом в информационную систему канала[1].

Овчинский В.С. выделяет несколько видов социальных объединений в сфере киберпреступности: хакерские сообществ, хактивисты, группы смерти, деструктивные секты[2].

Опасность участия преступных сообществ в совершении преступлений в сфере компьютерной информации не вызывает сомнения, данный квалифицирующий признак по праву закреплен в статьях УК Туркменистана, устанавливающих уголовную ответственность за преступления в сфере компьютерной информации. Мы считаем, что аналогичный квалифицирующий признак также стоит закрепить в преступлениях главы 28 УК РФ, поскольку, как показывает практика и вышеуказанные примеры, такая форма соучастия, как преступное сообщество, является актуальной формой объединения преступников с целью совершения ряда тяжких и особо тяжких преступлений по различным мотивам и единому умыслу.

Также следует обратить внимание на систему построения квалифицирующих признаков с формами соучастия в преступлениях, предусмотренных главой 28 УК РФ и главой 33 УК Туркменистана. Такой квалифицирующий признак в двух уголовных законодательствах построен следующим путем: «деяния, предусмотренные частями первой или второй настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой»[3]. Однако, как описано нами выше, уровень общественной опасности рассматриваемых форм преступного объединения

---

[1] См.: Хакеры могли предложить работнику ВГТРК за помощь до $1 млн. [Электронный ресурс]. URL: https://nsn.fm/policy/hakery-mogli-predlozhit-rabotniku-vgtrk-za-pomosch-do-1-mln (дата обращения: 7.10.2024).

[2] См.: Овчинский, В.С. Криминология цифрового мира: учебник для магистратуры / В.С. Овчинский. М. : Норма : ИНФРА-М, 2018. 352 с.

[3] Уголовный кодекс Туркменистана от 12 июня 1997 № 222-I. [Электронный ресурс]. URL: online.zakon.kz/Document/? Doc_id=3129586 (дата обращения: 07.10.2024); Уголовный Кодекс РФ от 13 июня 1996 № 63-ФЗ. [Электронный ресурс]. URL.: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения 26.10.2024).

имеет различные аспекты. Исходя из этого, по нашему мнению, квалифицирующие признаки с формами соучастия в преступлениях в сфере компьютерной информации следует разграничить и закрепить отдельными пунктами в рамках статей. За каждое из таких преступлений предусмотреть четкую уголовную ответственность в зависимости от уровня общественной опасности форм соучастия.

Следует также повысить уровень уголовного наказания за совершения преступлений в сфере компьютерной информации посредством соучастия. Это может быть сформулировано следующих образом: «Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные группой лиц по предварительному сговору, наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет, либо лишением свободы на тот же срок». И далее: «Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные организованной группой, наказываются ограничением свободы на срок до 6 лет, либо принудительными работами на срок до 7 лет, либо лишением свободы на тот же срок»[1].

Вытекающим обстоятельством, связанным с деятельностью преступного сообщества, являются тяжкие последствия, которые закреплены в преступлениях главы 28 УК РФ и главы 33 УК Туркменистана, предусмотренные п. 4 ст. 272 УК РФ, п.3 ст. 272 УК РФ, ч. 2 ст. 274 УК РФ, п. 3 ст. 374 УК Туркменистана, п. 3 ст. 376 УК Туркменистана, п. 3 ст. 379 УК Туркменистана, п.3 ст. 380 УК Туркменистана[2]. Толкование тяжких последствий имеет различия в зависимости от вида преступления, в случае

---

[1] Уголовный кодекс Туркменистана от 12 июня 1997 № 222-I. [Электронный ресурс]. URL: online.zakon.kz/Document/? Doc_id=3129586 (дата обращения: 07.10.2024); Уголовный Кодекс РФ от 13 июня 1996 № 63-ФЗ. [Электронный ресурс]. URL.: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения 22.05.2024).

[2] Уголовный кодекс Туркменистана от 12 июня 1997 № 222-I. [Электронный ресурс]. URL: online.zakon.kz/Document/? Doc_id=3129586 (дата обращения: 07.10.2024); Уголовный Кодекс РФ от 13 июня 1996 № 63-ФЗ. [Электронный ресурс]. URL.: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения 22.05.2024).

преступлений в сфере компьютерной информации тяжкие последствия имеют свою интерпретацию. Тяжкие последствия – это серьезные негативные последствия, причиненные личности, обществу, государству, которые возникают в результате противоправных действий субъекта преступления. Перечень таких тяжких последствий в рамках преступлений в сфере компьютерной информации является неисчерпаемым, основным компонентом определения тяжких последствий является масштаб противоправного воздействия, а также ценность материального либо нематериального компонентов для субъекта, владеющего данным компонентом. В соответствии с постановлением Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37 под тяжкими последствиями как квалифицирующим признаком понимается длительная приостановка работы предприятия, учреждения или организации, получение информации, составляющей охраняемую законом тайну, причинение по неосторожности смерти, тяжкого вреда здоровью и т.п.[1]. При квалификации преступления с тяжкими последствиями должна быть определена и доказана действительная угроза наступления тяжких последствий[2].

Кроме того, при рассмотрении тяжких последствий как квалифицирующего признака преступлений в сфере компьютерной информации следовало бы к таким последствиям отнести кражу банковских данных, взлом серверов государственных органов, предприятий, организаций, проникновение в систему организации и уничтожение данных, признанных государственной тайной, получение кодов доступа к информационной системе государственных органов с целью уничтожения либо модификации

---

[1] Постановление Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» //СПС«КонсультантПлюс». [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_434573/.

[2] См.: Там же.

информации, доступ к критической инфраструктуре государства и, как следствие, изменение ее работы.

Все вышеуказанные действия являются критически опасными и могут привести к необратимым последствиям, таким как завладение информацией, признанной государственной тайной, приостановка работы либо уничтожение информационной системы государства, а также к последствиям физического характера по отношению к личности и обществу.

В преступлениях, предусмотренных ст. 378 УК Туркменистана (распространение заведомо сфальсифицированной информации), содержится такой квалифицирующий признак, как совершение деяния при проведении массовых мероприятий и в условиях чрезвычайного и военного положения[1]. Согласно закону Туркменистана от 18.12.2013 № 456 – IV «О военном положении» под военным положением понимается «особый правовой режим деятельности органов государственной власти, органов местного самоуправления и юридических лиц независимо от их организационно-правовой формы и формы собственности (далее - юридические лица) и их должностных лиц, предусматривающий ограничение прав и свобод граждан, возложение на них дополнительных обязанностей, временно вводимый в соответствии с настоящим Законом на всей территории Туркменистана или в отдельных её местностях в случае военной угрозы, военного вмешательства во внутренние дела или осуществления против него вооружённой агрессии или возникновения её непосредственной угрозы для Туркменистана в целях обороны государства, обеспечения общественного порядка и национальной безопасности»[2].

Режим чрезвычайного положения также является особым правовым статусом, комплексом мер, принятых для предотвращения обстоятельств,

---

[1] Уголовный кодекс Туркменистана от 12 июня 1997 № 222-I. [Электронный ресурс]. URL: online.zakon.kz/Document/? Doc_id=3129586 (дата обращения: 07.10.2024).

[2] Закон Туркменистана от 18.12.2013 № 456 – IV «О военном положении». [Электронный ресурс]. URL: https://base.spinform.ru/show_doc.fwx?rgn=85288 (дата обращения: 09.10.2024).

ставших основанием его введения. В силу Закона Туркменистана от 22 июня 2013 г. № 412-IV под режимом чрезвычайного положения понимается «особый правовой режим деятельности органов государственной власти и местного самоуправления, юридических лиц независимо от их организационно-правовых форм и форм собственности, их должностных лиц, вводимый в соответствии с Конституцией Туркменистана и настоящим Законом на всей территории Туркменистана или в его отдельных местностях, допускающий установленные настоящим Законом отдельные ограничения прав и свобод граждан Туркменистана, иностранных граждан, лиц без гражданства, прав юридических лиц, а также возложение на них дополнительных обязанностей»[1]. Согласно ст. 12 данного закона на территории Туркменистана во время ведения военного положения вводятся ограничения на свободу печати в средствах массовой информации, а также изъятие технических средств, введение контроля за работой системы связи, вычислительных центров, запрещение работы абонентских радиостанций, любительских радиостанций[2].

Соответственно распространение сфальсифицированной информации через информационную систему может привести к особо тяжким последствиям в виде нарушения общественной безопасности, интересов личности и общества, а также интересов государства.

Военное положение — это режим особого правового поля с целью реализации мер безопасного функционирования не только вооруженных сил, но и всех критических систем государства, в том числе информационных систем, в связи с которым вводятся ограничения использования данных систем с целью предотвращения дестабилизации обстановки в государстве. Чрезвычайное положение также является режимом особого правового поля

---

[1] Закон Туркменистана от 22.06.2013 № 412 – IV «О режиме чрезвычайного положения». [Электронный ресурс]. URL: https://base.spinform.ru/show_doc.fwx?rgn=66001 (дата обращения: 09.10.2024).

[2] Закон Туркменистана от 22.06.2013 № 412 – IV «О режиме чрезвычайного положения». [Электронный ресурс]. URL: https://base.spinform.ru/show_doc.fwx?rgn=66001 (дата обращения: 09.10.2024).

с целью устранения чрезвычайных ситуаций природного и техногенного характера, а также ситуаций, связанных с насильственным изменением конституционного строя Туркменистана, массовыми беспорядками, террористическими актами и т.п[1]. Данный квалифицирующий признак является уместным в структуре ст. 378 УК Туркменистана, так как уровень последствий является критическим как для общества, так и для государства в целом.

В структуру действий по распространению сфальсифицированной информации во время чрезвычайного и военного положения входят распространение дезинформации и ложной пропаганды через информационно-телекоммуникационные сети, информационную систему телерадиовещания с целью подрыва доверия к государственным органам власти, вооруженным силам, а также призыва к совершению противоправных действий. Исходя из возможных противоправных действий, особо тяжкими последствиями следует считать дестабилизацию политической, экономической обстановки в государстве, нарушение общественной безопасности и т.п.

В связи с особым государственным статусом чрезвычайного и военного положения обеспечение безопасности информационной системы является одним из приоритетных направлений ввиду масштабной цифровизации государственных отраслей и налаживание бизнес-процессов через систему информационного взаимодействия, отсюда и критический уровень последствий в случае противоправного влияния на информационную инфраструктуру, в том числе нарушение правил обращения с компьютерной информацией. Данный особо квалифицирующий признак является также актуальным и для преступлений в сфере компьютерной информации по уголовному законодательству Российской Федерации.

---

[1] Закон Туркменистана от 22.06.2013 № 412 – IV «О режиме чрезвычайного положения». [Электронный ресурс]. URL: https://base.spinform.ru/show_doc.fwx?rgn=66001 (дата обращения: 09.10.2024).

Также целесообразно предусмотреть данный квалифицирующий признак (деяние, совершенное во время чрезвычайного и военного положения) в иных составах преступлений в сфере компьютерной информации, например, ст. 373, ст. 375-376, ст. 379-380, ст. 383 УК Туркменистана, аналогично в УК РФ ст. 272-274.1[1].

В соответствии с Законом Туркменистана от 28.02.2015 № 185-V массовое мероприятие – это открытое, мирное собрание, проводимое по инициативе граждан, политических партий, религиозных организаций с целью свободного выражения и формирования мнения по различным вопросам политического, культурного и экономического характера[2].

Обстоятельства массового характера имеют весьма рискованные последствия в случае попыток дестабилизации и расшатывания мирного собрания, поворота в противоправное русло. Такие попытки на практике часто осуществляются путем распространения сфальсифицированной информации, рассылающейся участникам массовых мероприятий, и в настоящее время не требуется осуществлять действия доведения информации физическим способом, довольно просто это сделать посредством информационно-телекоммуникационной сети. Попытка массового вовлечения людей в совершение противоправных действий является обстоятельством, существенно повышающим уровень опасности противоправного деяния по отношению к основному составу преступления (ст. 378 УК Туркменистана).

На основании вышеизложенного можно заключить, что особо квалифицирующие признаки преступлений в сфере компьютерной информации являются своего рода мерой правоохранительного толка, направленной на противодействие противоправным деяниям в данной сфере.

---

[1] Уголовный кодекс Туркменистана от 12 июня 1997 № 222-I. [Электронный ресурс]. URL: online.zakon.kz/Document/? Doc_id=3129586 (дата обращения: 07.10.2024); Уголовный Кодекс РФ от 13 июня 1996 № 63-ФЗ. [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения 22.05.2024).

[2] Закон Туркменистана от 28.02.2015 № 185 – V «Об организации и проведении собраний, митингов, демонстраций и других массовый мероприятий». [Электронный ресурс]. URL: https://online.zakon.kz/Document/?doc_id=31677936&pos=6;-106#pos=6;-106 (дата обращения: 9.10.2024).

Соотношения таких признаков по УК РФ и УК Туркменистана имеют равные значения, но присутствуют и индивидуальные признаки, являющиеся важными для каждой из рассматриваемых стран. Несмотря на то, что Российская Федерация еще в конце 20 века заложила основу в борьбе с компьютерными преступлениями, закрепив некоторые преступления в УК РФ, которые в последствии также были использованы в качестве основы противодействия инновационным на тот период общественным отношениям законодателем Туркменистана, УК Туркменистана и УК Российской Федерации активно развиваются и формируют свои принципиальные правовые позиции для обеспечения безопасности информационного пространства. Эти изменения видны в конструкционных особенностях таких составов, в том числе в особо квалифицирующих признаках, которые являются на сегодняшний день важными для правоприменителя индикаторами уровня общественной опасности противоправных действий.

Заключение[1]

Прогресс компьютерных технологий и использование их в противоправных целях не имеет смысла откладывать на плечи будущего мира, так как данная категория прогрессивного элемента цивилизационного развития диктует необходимость решения проблем противоправного использования новелл компьютерной отрасли уже в настоящее время, так как уже настоящее демонстрирует нам высокую динамику отрицательного прогресса влияния данных технологий на общественные отношения различной формации. Как отмечалось ранее, данный прогресс не замыкается в рамках территориальных границ государств, а имеет глобальный спектр охвата. Проведенное сравнительно-правовое исследование преступлений в сфере компьютерной информации по уголовному законодательству Российской Федерации и Туркменистана является своего рода дорожной картой по унификации двух уголовных законодательств в проблемной области, а также по оптимизации уголовно-правовых мер противодействия таким преступлениям.

В этом плане Российская Федерации и Туркменистан взяли курс на наведение порядка в информационном пространстве своих территориальных границ. Об этом свидетельствует увеличение числа нормативных правовых актов разной формации, таких как Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской

---

[1] См.: Корпеев, А.Г. Классификация преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (технологий), по уголовному законодательству Российской Федерации и Туркменистана // Юридический вестник Самарского университета Juridical Journal of Samara University. 2023. Т.9, № 4. С. 102–107; Корпеев, А.Г. Об объекте преступлений, совершаемых с использованием информационно-телекоммуникационных сетей, по уголовному законодательству России и Туркменистана // Юридический аналитический журнал. 2022. 17 (1). С. 29–33; Корпеев А.Г. О предмете преступлений, совершаемых с использованием информационно-телекоммуникационных сетей, по уголовному законодательству Российской Федерации и Туркменистана // Юридический аналитический журнал. 2023. 18 (1). С. 20-24; Корпеев, А.Г. Средства совершения преступлений в сфере компьютерной информации по уголовному законодательству Российской Федерации и Туркменистана // Юридический вестник Самарского университета Juridical Journal of Samara University. 2025. Т. 12, № 2. С.96-102.

Федерации»[1], Закон Туркменистана «О кибербезопасности» от 2019 года, не говоря уже об основных законах страны в сфере обеспечения защиты информации, таких как Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[2]; Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи»[3]; Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»[4], Закон Туркменистана от 3 мая 2014 года № 72-V «Об информации и её защите»[5]; Закон Туркменистана от 20 декабря 2014 года № 159-V «О правовом регулировании развития сети Интернет и оказания интернет-услуг в Туркменистане»[6]. Наполнение законодательной базы в сфере информационной безопасности показывает систематизационную направленность двух государств к достижению поставленных целей.

При всем генезисе нормотворчества имеются упущения в рамках уголовно-правовой регламентации преступлений в сфере компьютерной информации. Как показывает практика, уголовное законодательство не поспевает за новыми трендами в сфере информационных технологий, а связано это в первую очередь с изысканием компонентов такого «тренда», в том числе с определением понятийного аппарата, сущности возможностей, с определением угроз системе информационной безопасности.

Важно заметить, что в период с 1997 года, с момента принятия Уголовного кодекса Туркменистана, система построения положений о преступлениях в сфере компьютерной информации была идентична

---

[1] Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». [Электронный ресурс]. URL: https://base.garant.ru/71556224/.

[2] Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ. [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_61798/

[3] Федеральный закон «Об электронной подписи» от 06.04.2011 № 63-ФЗ. [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_112701/

[4] Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ. [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_61801/

[5] Закон Туркменистана от 3 мая 2014 года № 72-V «Об информации и её защите». [Электронный ресурс]. URL: https://online.zakon.kz/Document/?doc_id=34731231

[6] Закон Туркменистана от 20 декабря 2014 года № 159-V «О правовом регулировании развития сети Интернет и оказания интернет-услуг в Туркменистане. [Электронный ресурс]. URL: https://online.zakon.kz/Document/?doc_id=31648447

положению таких составов в системе Уголовного кодекса Российской Федерации. Однако с 2022 года в Туркменистане произошли масштабные изменения положений Уголовного кодекса, в том числе была реформирована и глава 33 «Преступления в сфере компьютерной информации». Во-первых, в Уголовном кодексе Туркменистана была кардинально перестроена система расположения преступлений в сфере компьютерной информации. Основное нововведение, отличное от Уголовного кодекса России, было связано с введением нового раздела III «Преступления в сфере компьютерной информации» и главы XXXIII с креативным названием «Преступления в сфере информатики и связи». Глава была наполнена 11 новыми составами преступлений, отличными от Уголовного кодекса Российской Федерации[1].

При этом мы считаем, что название раздела и главы являются некорректными с точки зрения логики и науки. Информатика – это целая наука, которая изучает процессы и методологию, связанные с возможностью передачи информации. Эта наука включает себя широкий спектр дисциплин, изучающих различные компоненты информации, включая ~~изучение~~ передачу, обработку, хранение компьютерной информации. Поэтому, когда мы говорим об информатике и компьютерной информации, следует подразумевать соотношение рода и вида. В связи с этим понятно, что по уровню иерархичности наука выше, чем дисциплина науки. Исходя из этого, предлагается внести изменения в Уголовный кодекс Туркменистана путем перестановки названий раздела и главы.

Среди других вопросов модернизации Уголовного кодекса Туркменистана, рассматриваемых в научном исследовании, следует выделить отсутствие понятийно-категориального аппарата, в отличие от Уголовного кодекса Российской Федерации. Например, в Уголовном кодексе

---

[1] Корпеев А.Г. Классификация преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (технологий), по уголовному законодательству Российской Федерации и Туркменистана // Юридический вестник Самарского университета Juridical Journal of Samara University. 2023. Т.9, № 4. С. 102–107.

Туркменистана отсутствуют важные, по нашему мнению, для установления объективной стороны понятия «компьютерная информация» и использованное в статьях кодекса «охраняемая законом информация». В связи с этим нами предложено закрепить понятие компьютерной информации и охраняемой законом информации в конструкции ст. 373 УК Туркменистана и понимать под компьютерной информацией электронную информацию (имеющую вид текстового, числового, звукового и графического содержания), представленную в символьной форме, содержащуюся на материальных электронно-вычислительных носителях, а также различных информационно-телекоммуникационных сетях связи. Под охраняемой законом информацией следует понимать информацию, для которой установлен особый статус правовой защиты действующим законодательством Туркменистана. Вместе с тем особый статус правовой защиты такой информации предусматривает специальные правила ее хранения, обработки и распространения в целях обеспечения ее конфиденциальности.

Также теоретика-прикладные основы Российской Федерации и Туркменистан требуют решения вопроса правовой природы объекта, предмета, способов, а также средств совершения. К числу предметов таких преступлений следует относить компьютерную информацию и национальную критическую информационную инфраструктуру. Средствами совершения данных деликтов следует определять триады материальных и нематериальных средств: вредоносные программы, средства связи, компьютерные устройства. К числу способов совершения относится септет различных противоправных манипуляций в сфере компьютерной информации. Спецификой определения природы объекта таких деликтов следует признавать наличие основного и дополнительного объектов – информационной безопасности.

Другим упущением следует признать, что в практической сфере Туркменистана отсутствуют ориентиры применения положений Уголовного кодекса Туркменистана о преступлениях в сфере компьютерной информации.

По нашему мнению, уже давно назрела необходимость разъяснения со стороны судебной власти применения норм о преступлениях в сфере компьютерной информации в ввиду специфичности самой сферы, требующей детального понимая технической составляющей многими правоприменителями. Кроме того, важной составляющей в данном случае является способствование унификации подходов к применению норм о преступлениях в сфере компьютерной информации на территории Туркменистана. В связи с этим нами разработано и предложено для использования постановление Пленума Верховного Суда Туркменистана «О некоторых вопросах, возникающих у судов при рассмотрении уголовных дел о преступлениях в сфере компьютерной информации». С нашей точки зрения такое постановление оптимизирует правоприменительную практику с точки зрения уточнения важных аспектов использования компьютерной информации.

Новоиспеченный уголовный законодательный постмодернизм требует смелых решений в виде реформирования Уголовного законодательства Туркменистана. Сегодня с учетом динамично возрастающих «цифровых» имущественных отношений, в которых переплетаются две категории общественной жизни - информационные и экономические, появления цифровых имущественных благ в виде цифровых ценных бумаг, валюты приводят к совершению преступлений в данной сфере. К тому же увеличение числа цифровых имущественных преступлений сподвигает нас предложить введение новой статьи – 249[1] «Хищение в сфере цифровых технологий».

«Мы должны быть рабами закона, чтобы стать свободными»[1]. В этой цитате, по нашему мнению, прослеживается смысловой посыл того, что общественные действия человека должны быть согласованы с законом,

---

[1] Марк Туллий Цицерон Из речи в защиту Клуенция. Legum … servi sumus ut liberi esse possimus. [Электронный ресурс]. URL: https://ru.citaty.net/tsitaty/457359-mark-tullii-tsitseron-my-dolzhny-byt-rabami-zakonov-chtoby-stat-svobodn/ (дата обращения: 06.02.2025).

порядок любых взаимоотношений в государстве строится на основе определенных законодательных правил. В этом смысле область компьютерных преступлений остается необъятной, а многие отношения в сфере компьютерной информации остаются за пределами взора уголовного законодательства. Именно поэтому уголовное законодательство Российской Федерации требует свежего глотка новелл в части цифровых преступлений. Подход к обращению с компьютерной информацией требует жестких мер для обеспечения свободных отношений в информационной сфере. Цифровые преступления в системе уголовного права России давно не видели инновационного подхода, а если быть точным, то с самого своего появления - с 1997 года - в структуре уголовного закона практически не подвергались существенным изменениям. Изменение уголовно-правовой формации в сторону открытия новых видов преступных посягательств в цифровом пространстве наталкивают на давно обсуждающуюся в научной литературе смену научной парадигмы. Все материи с автоматическим вычислением опасны, взор в будущее является откладыванием существующих реалий в долгий ящик, ведь будущее уже тут, просто мы его пытаемся не видеть. В этом смысле в работе представлен комплекс модернистских предложений по наполнению главы 28 УК РФ «Преступления в сфере компьютерной информации». В частности, предлагаем дополнить статью 274^3 «Неправомерная модификация программного обеспечения беспилотных систем». Сфера использования беспилотного транспорта вышла на плато своего развития, применение таких средств в процессе модификации угрожает обеспечению общественного порядка, а также грозит причинением вреда здоровью человека.

Ввиду распространения случаев применения насилия (психического и физического) с целью получения компьютерной информации (обычно такие методы используют к людям, обладающим разрешительным доступом к

охраняемой законом информации), предлагается ввести статью 272^2 «Принуждение к передаче информации».

В совокупности вышеуказанные новеллы помогут оптимизировать:

- контроль за применением беспилотного транспорта;
- дополнительно сферу безопасности общественного порядка, а также защиту граждан;
- обеспечение дополнительной безопасности охраняемой законом информации;
- обеспечение защиты субъектов, осуществляющих контроль за хранением, обработку и передачу информации.

Нормотворческая деятельность, если она движется в соприкосновении со временем, действительно является важным стимулирующим фактором на пути к свободе безопасного использования технологических новаторств.

Наше исследование в данном случае является одним небольшим шагом к новаторству цифровой безопасности. Технологии именуются по-разному, безопасность обозначается как информационная, цифровая, технологическая, однако суть одна - определение уголовно-правых ориентиров на пути к решению вопросов безопасного существования человека в цифровых реалиях.

Исходя из вышеперечисленных результатов, можно сделать выводы:

1. Уголовно-правовая политика Российской Федерации и Туркменистана в сфере регулирования цифровых отношений и защиты информации находится в мобилизационном положении.

2. Уголовный кодекс Туркменистана имеет отличительные особенности от уголовного кодекса Российской Федерации в системе содержания положений о преступлениях в сфере компьютерной информации; в первом случае создан целый раздел, имеется разнообразие видов преступлений.

3. В уголовном кодексе Туркменистана в части преступлений в сфере компьютерной информации выявлены проблемы понятийно-категориального

аппарата, в этом направлении предложены определенные варианты решения проблемы.

4. Определены единые подходы в понимании средств совершения преступлений в сфере компьютерной информации путем нашего предложения по выделению «триады» таких средств.

5. В вопросе понятийно-категориального аппарата определена терминология обозначения различных видов преступлений в сфере компьютерной информации и иных преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, под единым термином «компьютерные преступления».

6. Рассмотрен вопрос правовой сущности термина «киберпреступность», обозначено, что данный термин является криминологической, а не уголовно-правовой категорией. Обосновано данное утверждение тем, что сущность термина является в определении ситуационных и социологических особенностях общественно опасных деликтов. Термин является собирательным выражением совокупности определенных явлений в цифровом пространстве.

7. Выработаны и предложены существенные изменения в уголовное законодательство Российской Федерации и Туркменистана, а также разработаны предложения с целью унификации судебной практики по уголовным делам о преступлениях в сфере компьютерной информации в Туркменистане.

8. Уголовные кодексы Российской Федерации и Туркменистана имеют ряд противоположных подходов в вопросах регулирования общественных отношений в сфере компьютерной информации, однако существуют унифицированные подходы, регламентирующиеся внутренним законодательством двух стран, в том числе выработаны единые пути по борьбе с компьютерными преступлениями на региональном уровне в рамках СНГ и на международном уровне.

Возвращаясь к вопросу трансграничности компьютерных преступлений, необходимо отметить, что процесс технологического развития, появление новых способов совершения таких преступлений действительно заставляет задуматься об унификации уголовного законодательства Российской Федерации и Туркменистана в части регулирования общественных отношений в сфере компьютерной информации, государств соседей, стратегических партнеров, а также участников исторических событий, связывающих две страны в единый исторический период. Вопросы настоящего и будущего, возникающие в сфере цифровых отношений, всегда будут упираться в определённые государственные границы, а также внутреннее законодательство, но тем не менее задачи по исследованию многообразия лучших практик, а также поиск лучших подходов путем сравнения, и как результат имплементация лучших подходов в законодательство своей страны является определяющим фактором, способным выявить единые подходы в борьбе с компьютерной преступностью. С учетом сказанного следует и далее продолжать научные изыскания в сфере развития уголовного законодательства Российской Федерации и Туркменистана с целью научного поиска оптимальной модели унификации двух законодательств, а также гармонизации внутреннего права и переосмысления определённых мер, принимаемых с целью противодействия компьютерным преступлениям.

Список литературы

Международные нормативные правовые акты

1. Конвенции ООН об обеспечении международной информационной безопасности [Электронный ресурс]. URL: https://namib.online/wp-content/uploads/2020/04/%D0%9A.
2. Конвенция Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях принята 27 ноября 2024 года. [Электронный ресурс]. URL:https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Russia_Contribution_R.pdf /.
3. Конвенция против киберпреступности; Укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям, принята резолюцией 79/243 Генеральной Ассамблеей от 24 декабря 2024 года. [Электронный ресурс]. URL: https://www.un.org/ru/documents/treaty/A-RES-79-243.
4. Резолюции Генеральной Ассамблеи Организация Объединенных Наций A/RES/64/211 от 21 декабря 2009 г. «Создание глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших информационных инфраструктур» [Электронный ресурс]. URL: https://online.zakon.kz/Document/?doc_id=31602038.
5. Резолюцию Генеральной Ассамблеи Организации Объединенных Наций A/RES/55/29 от 20 ноября 2000 г. «Роль науки и техники в контексте международной безопасности и разоружения». [Электронный ресурс]. URL:https://www.un.org/ru/ga/55/docs/55res1.shtml.
6. Резолюцию Генеральной Ассамблеи Организации Объединенных Наций A/RES/65/41 от 8 декабря 2010 г. «Достижения в сфере

информатизации и коммуникаций в контексте международной безопасности» [Электронный ресурс]. URL: https://online.zakon.kz/Document/?doc_id=31094419

7. Конвенция о преступности в сфере компьютерной информации от 23 ноября 2001 года ETS № 185 // ЭПС «Система ГАРАНТ». [Электронный ресурс]. URL: http://base.garant.ru/4089723/#ixzz5WwK9w8it (дата обращения: 13.08.2023).
8. Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в области обеспечения информационной безопасности от 20.11.2013 // СПС «Консультант Плюс». [Электронный ресурс]. URL: https://docs.cntd.ru/document/420278452.
9. Соглашение между Правительством Российской Федерации и Правительством Туркменистана «О сотрудничестве в области обеспечения международной информационной безопасности» от 05.04.2019. [Электронный ресурс]. URL: https://www.mid.ru/ru/foreign_policy/international_contracts/international_contracts/2_contract/56086/.

Нормативные правовые акты
Российской Федерации и Туркменистана

10. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020). [Электронный документ]. URL: https://www.consultant.ru/document/cons_doc_LAW_28399/

11. Конституция Туркменистана (новая редакция принята 14 сентября 2016 года). [Электронный документ]. URL: https://turkmenistan.gov.tm/ru/post/69352/konstitucionnyj-zakon-turkmenistana.

12. Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 № 230-ФЗ // Собрание законодательства РФ. – 25.12.2006. – № 52.

13. Уголовный Кодекс РФ от 13 июня 1996 № 63-ФЗ // Собрание законодательства РФ. – 1996. – № 25.

14. Уголовный Кодекс РФ от 13 июня 1996 № 63-ФЗ. [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_10699/.

15. Уголовный Кодекс Туркменистана от 12 июня 1997 № 222-I. [Электронный документ]. URL: online.zakon.kz/Document/? Doc_id=3129586.

16. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Российская газета. – 29.07.2006. – № 165.

17. Закон Туркменистана от 18.12.2013 № 456 – IV «О военном положении». [Электронный документ].URL: https://base.spinform.ru/show_doc. fwx?rgn=85288.

18. Закон Туркменистана от 22.06.2013 № 412 – IV «О режиме чрезвычайного положения». [Электронный документ]. URL. https://base.spinform.ru/show_doc.fwx?rgn=66001 (дата обращения: 09.10.2024)

19. Закон Туркменистана «Об информации и ее защите» от 3.05.2014 года № 72V. [Электронный документ]. URL: https://online.zakon.kz/Document/?doc_id=34731231 (дата обращения 23.01.2024).

20. Закон о кибербезопасности Туркменистана от 07.09.2019. [Электронный документ]. URL: https://turkmenportal.com/blog/21542/v-turkmenistane-podgotovlen-proekt zakona-o-kiberbezopasnosti (дата обращения: 22.01.2024).

21. Закон Туркменистана «О правовом регулировании развития сети Интернет и оказания интернет – услуг в Туркменистане» от 20.12.2014 №159-V. [Электронный документ]. URL: https://www.parahat.info/law/2014-12-29-zakon-turkmenistana-o-pravovom-regulirovanii-razvitiya-seti-internet-i-okazaniya-internet-uslug-v-turkmenistane.

22. Закон Туркменистана от 28.02.2015 № 185 – V «Об организации и проведении собраний, митингов, демонстраций и других массовый мероприятий». [Электронный документ]. URL. https://online.zakon.kz/Document/?doc_id=31677936&pos=6;-106#pos=6;-106.

23. Меры по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена, утвержденные Указом Президента РФ от 17.03.2008 № 351. [Электронный документ]. URL: https://www.consultant.ru/document/cons_doc_LAW_75586/.

24. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 5.12.2016 № 646). [Электронный документ]. URL: https://www.consultant.ru/document/cons_doc_LAW_208191/ (дата обращения 21.01.2025).

25. Основы государственной политики Российской Федерации в области международной информационной безопасности, утверждены Указом Президента России от 12.04.2021 № 213. [Электронный документ]. URL:http://static.kremlin.ru/media/events/files/ru/RR5NtCWkkZPTuc5TrdHURpA4vpN5UTwM.pdf.

26. Стратегия национальной безопасности Российской Федерации (утв. Указом Президента РФ от 2.07.2021 № 400). [Электронный документ]. URL: https://www.mid.ru/ru/foreign_policy/official_documents/1784948/.

27. Стратегия развития информационного общества в Российской Федерации на 2017 – 2030 годы, утвержденной Указом Президента РФ от 9.05.2017 № 203. [Электронный документ]. // URL: tps://base.garant.ru/71670570/.

28. Основы государственной политики Российской Федерации в области международной информационной безопасности, утвержденные Указом Президента РФ от 12 апреля 2021 г. № 213. СПС «КонсультантПлюс». [Электронный документ].

URL:http://www.consultant.ru/document/cons_doc_LAW_381999/9bbf31c7586971ae3d3076bfb49080d41d6c4484.

29. Постановление об обеспечении кибербезопасности, утвержденное Президентом Туркменистана от 19.01.2024. [Электронный документ]. URL: https://asmannews.ru/news/2194/prezident-turkmenistana-podpisal-postanovlenie-ob-obespecenii-kiberbezopasnosti.

30. Государственная программа по обеспечению кибербезопасности Туркменистана на 2022-2025 г., утвержденная Президентом Туркменистана от 02.03.2022 № 2623. [Электронный документ]. URL: https://turkmen.news/wp-content/uploads/2022/09.

31. Письмо Минцифры России от 27.01.2022 № П11-2-05-200-3571 «О рассмотрении обращений субъектов предпринимательской деятельности и заинтересованных лиц в сфере информационных технологий». [Электронный документ]. URL: https://www.consultant.ru/document/cons_doc_LAW_408074/.

Судебные акты

32. Постановление Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» //СПС«КонсультантПлюс». [Электронный ресурс]. URL:https://www.consultant.ru/document/cons_doc_LAW_43457.

33. Постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет». [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_434573/.

34. Постановление Пленума Верховного Суда РФ от 10.06.2010 N 12 «О судебной практике рассмотрения уголовных дел об организации преступного сообщества (преступной организации) или участии в нем (ней)». [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_101362/ (дата обращения: 07.10.2025).

35. Постановление Пленума Верховного Суда РФ от 27.01.1999 N 1 (ред. от 03.03.2015) «О судебной практике по делам об убийстве (ст. 105 УК РФ)» [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_21893/.

36. Приговор Буденовского городского суда от 04.10.2012 по делу № 1-405/2012// [Электронный ресурс]. URL: https://budenovsky.stv.sudrf.ru/.

37. Приговор Клининского городского суда Московской области от 25.09.2014 № 1-275/14. [Электронный ресурс] – Режим доступа - URL: https://klin.mo.sudrf.ru/.

38. Приговор Головинского районного суда г. Москва от 25 мая 2023 года по делу № 1-342/2023. [Электронный ресурс]. URL: https://mos-gorsud.ru/rs/golovinskij/services/cases/criminal/details/9959a360-e5c5-11ed-a575-f7b7b38a87de?caseNumber=1-342/2023.

39. Приговор Чкаловского районного суда города Екатеринбург от 07.06.2017 по делу № 1-609/2017. [Электронный ресурс]. URL: https://sud-praktika.cloud/precedent/420329.html.

40. Приговор Тушинского районного суда Москвы от 26.06.2020 № № 1-420/20. [Электронный ресурс]. URL: https://www.mos-gorsud.ru/rs/tushinskij/cases/docs/content/b69a423b-520c-43ba-91ad1f0dedbc7c86

41. Приговор Коминтерновского районного суда г. Воронеж от 24 апреля 2017 года по делу № 1-271/2017. [Электронный ресурс]. URL: https://advocate-service.ru/sud-praktika.html.

42. Приговор Комсомольского районного суда г. Тольятти Самарской области № 1-242/2021 от 23 июля 2021 года по делу № 1-242/2021. [Электронный ресурс]. URL: https://sudact.ru/regular/doc/7GwYuFr5wOog/.

43. Приговор Советского районного суда города Самара от 13.02.2017 по делу № 1-61/2017. [Электронный ресурс]. URL: https://sud-praktika.cloud/precedent/203577.html).

44. Приговор Автозаводского районного суда г. Тольятти Самарской области № 1-656/2021 от 26 июля 2021 года по делу № 1-656/2021. [Электронный ресурс]. URL: https://sudact.ru/regular/doc/ZazqFf6KGXoQ/.

45. Приговор Ленинского районного суда города Севастополь № 1-362/2023 от 18 сентября 2023 года по делу № 1-362/2023. [Электронный ресурс]. URL: https://sudact.ru/regular/doc/B47GXnZWo1WN/.

46. Приговор Октябрьского районного суда г. Ростов-на-Дону № 1-470/2023 от 15 сентября 2023 года по делу № 1-470/2023 . [Электронный ресурс]. URL: https://sudact.ru/regular/doc/RrV7B2BPCtZX/.

47. Приговор Мещанского районного суда г. Москвы от 19 мая 2017 года. [Электронный ресурс]. URL: https://mos-gorsud.ru/rs/meshchanskij.

48. Приговор Симоновского суда г. Москвы, от 18 мая 2022 № 1-124/22. [Электронный ресурс]. URL: https://mos-gorsud.ru/rs/simonovskij/cases/docs/co.

49. Приговор Чкаловского районного суда г. Екатеринбург, от 07 августа 2017 года № 1-609/17. [Электронный ресурс]. URL: https://sud-praktika.cloud/precedent/420329.html.

50. Приговор Коптевского районного суда г. Москвы, от 06 июня 2018 года № 1-121/18. [Электронный ресурс]. URL: https://www.mos-gorsud.ru/rs/koptevskij/cases/docs/.

51. Приговор Промышленного районного суда г. Самары № 1-87/2017 от 2017 года. [Электронный ресурс]. URL: https://sud-praktika.cloud/precedent/201301.html.

52. Приговор Коминтерновского районного суда г.Воронеж от 27.04.2017 № 1-271-2015. [Электронный ресурс]. URL: https://sud-praktika.cloud/precedent/546205.html.

53. Приговор Заельцовского районного суда г. Новосибирск от 11.07.2017 № 1-283-2017. [Электронный ресурс]. URL: https://sud-praktika.cloud/precedent/339721.html.

54. Приговор Центрального районного суда г. Челябинск от 27.02.2017 № 1-141/2017. [Электронный ресурс]. URL: https://sud-praktika.cloud/precedent/256261.html.

55. Приговор Лефортовского районного суда г. Москвы от 29.09.2016 № 1-277/2014. [Электронный ресурс]. URL: https://advocate-service.ru/sud-praktika/ugolovnye-dela/prigovory-sudov-po-st.-274.

56. Приговор Нагатинского районного суда г. Москвы от 29.09.2016 № 1-499/18. [Электронный ресурс]. URL: https://mos-gorsud.ru/rs/nagatinskij/cases/docs/content/6169dfc5-e25b-4b7e-9523-39a0d9ebca4f .

Иностранные источники

57. Chung L., Tan K.H. The unique Chinese innovation pathways: Lessons from Chinese small and medium sized manufacturing firms // International Journal of Production Economics. 2017. Vol. 190. P. 80–87.

58. Varese, F. Organized Crime: Critical Concepts in Criminology (London , Routledge , 2010) vol I. P. 11 – 33.

59. Varese, F. (ed), What is Organised Crime? vol I . P. 27 – 55. [Электронный ресурс]. URL: https://federicovarese.com/wp-content/uploads/2019/07/varese-2017-redefining-organised-crime-03.pdf (дата обращения: 19.01.2024).

60. Kingston, K.C. Artificial Intelligence and Legal Liability. Research and Development in Intelligent Systems XXXIII: Incorporating Applications and Innovations in Intelligent Systems XXIV // Cambridge: Springer. 2016. P. 269–279.

61. Neff P. N. Talking To Bots: Symbiotic Agency and the Case of Tay// International Journal of Communication. 2016. No.10. P. 4915–4931.

62. Yin Z., Xue G., Guo P. The Impact of Mobile Payment on Entrepreneurship – Micro Evidence from China Household Finance Survey // China Industrial Economics. – 2019. – № 3. P. 119–137.

63. Кэрриэ Б. Криминалистический анализ файловых систем [перевод] / Брайан Кэрриэ. — Санкт-Петербург: Питер, 2007. — 479 с.

64. Luttgens, Jason, Pepe Matthew, Mandia Kevin. Incident response & computer forensics, third edition // McGraw-Hill. – 2014. – 624 с.

Учебные пособия и научные статьи

65. Авдеев, М.А., Штранц, А.С. Общая характеристика квалифицирующих признаков и их значение при конструировании составов преступлений// Актуальные проблемы государства и права. 2019. Т. 3. № 9. С. 66 – 71.

66. Агешкина, Н.А., Беляев, М.А., Белянинова, Ю.В., Бирюкова Т.А., Болдырев С.А., Буранов Г.К., Воробьев Н.И., Галкин В.А., Дудко Д.А., Егоров Ю.В., Захарова Ю.Б., Копьёв А.В. Научно-практический комментарий к Уголовному кодексу Российской Федерации от 13 июня 1996 г. № 63-ФЗ. [Электронный ресурс]. URL: https://base.garant.ru/57227409/.

67. Аминов, И.И. Цивилистический обычай в правовой системе Туркменистана // Юрист. 2022. № 7. С. 8 – 13.

68. Антонов, А.Г., Зорина Е.А., Крюков, Д.В. К вопросу об общественной опасности неправомерного доступа к компьютерной информации // Вестник Томского государственного университета. Право. 2022. № 44. С. 5-16.

69. Батурин, Ю.М. Проблемы компьютерного права / Ю. М. Батурин. – Москва: Юридическая литература, 1991. - 272 с.

70. Бегишев, И. Р. Преступления в сфере обращения цифровой информации/ И.Р.Бегишев, И.И. Бикеев – Казань: Изд-во «Познание» Казанского инновационного университета, 2020. – 300 с.

71. И.Р. Бегишев, З.И. Хисамова, С.Г. Никитин. Организация хакерского сообщества: криминологический и уголовно-правовой аспекты // Всероссийский криминологический журнал. 2020. Т.14, №1. С.96-105.

72. Безверхов, А.Г. О предмете имущественных преступлений // Юридический вестник Самарского университета, 2017. № 4. С. 74-79.

73. Безверхов, А.Г. Закон и право в условиях цифровой экономики / А.Г. Безверхов // Государство и право: вопросы методологии, истории, теории и практики функционирования. - Самара: Изд-во Самар. ун-та. 2022. С. 14-30.

74. Бикмурзин, М.П. Предмет преступления: теоретико-правовой анализ. Москва: Юрлитинформ, 2006. — 184 с.

75. Бородин, С.В. Ответственность за убийство: квалификация и наказание по российскому праву. М.: Юрист,1994. - 216 с.

76. Бородин, С.В. Преступления против жизни. С.-Пб.: Юрид. центр Пресс, 2003. - 467 с.

77. Бражников С.Д. Преступления в сфере компьютерной информации: Учебно-метод. разработка по спецкурсу / Сост. С.Д. Бражников; Яросл. гос. ун-т. Ярославль, 2000. - 54 с.

78. Буликеева Д.Ж. Понятие и природа квалифицирующих признаков // Вестник Челябинского государственного университета. 2013 № 11. С. 68-71.

79. Быков, В.М. Признаки организованной преступной группы // Законность. 1998. №9. С. 4-8.

80. Вехов, В. Б. Компьютерные преступления: Способы совершения. Методики расследования / В. Б. Вехов. – Москва: Право и закон, 1996. – 182 с.

81. Витвицкая, С. С. Киберпреступления: понятие, классификация, международное противодействие / С. С. Витвицкая, А. А. Витвицкий, Ю. И. Исакова // // Правовой порядок и правовые ценности. — Т.1. № 1. С. 18–27.

82. Волеводз А.Г. Российское законодательство об уголовной ответственности за преступления в сфере компьютерной информации / А.Г. Волеводз // Российский судья, 2002. № 9. С. 34–41.

83. Горбунова, Л.В. Обстоятельства, отягчающие наказание. Их значение и соотношение с квалифицирующими признаками// Марийский юридический вестник. 2015. № 2. С. 40-46.

84. Губин, М.С. Преступления в сети Интернет. Учебное пособие / М. С. Губин — «Издательские решения», 2020. - 9 с.

85. Предсказания фантастов, сбывшиеся в технологиях (Из книги Джона Браннера «Оседлавший волну шока». 1975). [Электронный ресурс]. URL: https://myatom.ru/metromozg/prognoz/.

86. Джафарли, В. Ф. Криминологическая кибербезопасность: теоретические, правовые и технологические основы / В. Ф. Джафарли. – 2-е издание, переработанное и дополненное. – Москва: Общество с ограниченной ответственностью «Проспект», 2024. – 480 с.

87. Дорошков В.В. Комментарий к Уголовному кодексу Российской Федерации (отв. ред. В.М. Лебедев) / Г.Н. Борзенков, В.П. Верин, Б.В. Волженкин, А.В. Галахова, В.В. Демидов, В.В. Дорошков, Э.Н. Жевлаков, А.Н. Игнатов, М.М. Карелина, Е.П. Кудрявцева // М.: Юрайт, 2010. – 910 с.

88. Дубровский, Д.И. Идеальное как информация, непосредственно «данная» личности // Управление, информация, интеллект. М., 1976. С. 236.

89. Евдокимов, К.Н. Субъективная сторона неправомерного доступа // Вестник Академии Генеральной Прокуратуры РФ М. 2009 №12. С. 53-57.

90. Ефремова, М. А. Уголовная ответственность за преступления, совершаемые с использованием информационно-телекоммуникационных технологий. - М.: Юрлитинформ, 2015. – 200 с.

91. Журавлев М.П., Наумов, А.В. Уголовное право России. Части Общая и Особенная. Москва: Проспект: учебник / под ред. А. И. Рарога - Москва : Проспект, 2018. - 944 с.

92. Завадский, И.И. Информационная война – что это такое? // Конфидент. 1996. № 4. С. 13-15.

93. Иванова, Л.В. Виды киберпреступлений по российскому уголовному законодательству. Юридические исследования, 2019. С. 25-33.

94. Исахов, Ж.И. Субъективные ошибки и квалификация доведения до самоубийства путем самосожжения (по материалам Республики Казахстан). // Вестник Алтайской академии экономики и права. 2022. № 9. С. 274-277.

95. Кабурнеев, Э.В. Понятие квалифицирующих признаков и их роль в дифференциации уголовной ответственности за убийство // Законы России. 2007. № 4. С. 70 – 73.

96. Клишков, В.Б., Стебенева, Е.В., Яковлев М.А. Киберпреступность: понятие, признаки, основные направления противодействия // Вестник Нижегородского университета им. Н.И. Лобачевского, 2022, 4. С.111.

97. Князьков, А.А. Теория и практика квалификации преступлений: учебное пособие / А.А. Князьков; Яросл. гос. ун-т им. П. Г. Демидова. — Ярославль : ЯрГУ, 2018. — 100 с.

98. Кобец, П.Н. Характеристика особо квалифицирующих признаков состава разбоя по действующему законодательству // Символ науки, 2015. С.71-72.

99. Капитонова О.С. Понятие организованной группы // Криминалистъ, 2012. С. 23-26.

100. Козаев, Н.Ш. Состояние уголовной политики и вопросы преодоления кризисных явлений в уголовном праве // Юридический вестник ДГУ. 2016. №1. С. 96–101.

101. Комментарий к Уголовному кодексу Российской Федерации (научно-практический, постатейный). 6-е изд., перераб. и доп. / под ред. профессора Н.Г. Кадникова. – М.: ИД «Юриспруденция», 2019. – 1096 с.

102. Комментарий к Уголовному кодексу Российской Федерации / Отв. ред. А.И. Рарог. М.: Проспект, 2004. – 639 с.

103. Корпеев, А.Г. О предмете преступлений, совершаемых с использованием информационно-телекоммуникационных сетей, по уголовному законодательству Российской Федерации и Туркменистана». Юридический аналитический журнал. 2023. 18 (1). С. 20-24.

104. Корпеев, А.Г. Об объекте преступлений, совершаемых с использованием информационно-телекоммуникационных сетей, по уголовному законодательству России и Туркменистана». Юридический аналитический журнал. 2022. 17 (1). С. 29–33.

105. Корпеев, А.Г. Классификация преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (технологий), по уголовному законодательству Российской Федерации и Туркменистана // Юридический вестник Самарского университета Juridical Journal of Samara University. 2023. Т.9, № 4. С. 102–107.

106. Корпеев, А.Г. О квалифицирующих признаках преступлений в сфере компьютерной информации по уголовному законодательству России и Туркменистана // Вестник ТГУПБП. 2024. №1. С. 29-36.

107. Корпеев, А.Г. О субъекте преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (технологий), по уголовному законодательству Российской Федерации и Туркменистана // Вопросы российского и международного права. 2024. Том 1. № 1А. С. 354-363.

108. Корпеев, А.Г. Состояние и динамика преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (технологий), и в сфере компьютерной информации в Российской Федерации и

Туркменистане // Евразийский юридический журнал. 2024. № 2 (189). С. 342-344.

109. Корпеев, А.Г. Средства совершения преступлений в сфере компьютерной информации по уголовному законодательству Российской Федерации и Туркменистана // Юридический вестник Самарского университета Juridical Journal of Samara University. 2025. Т. 11, № 2. С. 96-102.

110. Кочкина, Э.Л. Определение понятия «киберпреступление» Отдельные виды киберпреступлений // Сибирские уголовно-процессуальные и криминалистические чтения 3: 2017. С. 162 – 169.

111. Кочои, С., Савельев, Д. Ответственность за неправомерный доступ к компьютерной информации // Российская юстиция, 1999. [Электронный ресурс] URL.: https://base.garant.ru/3540854/ (дата обращения 1.04.2024).

112. Кубиевич, С.В. IT-технологии в борьбе с преступностью // Роль бизнеса в трансформации общества. 2023. № 2. С. 450–454.

113. Куликова, С.А. Недостоверная информация как один из видов вредной информации: анализ правовой природы и систематизация // Известия Саратовского университета. Новая серия. Серия: Экономика. Управление. Право. 2013. С. 705-710.

114. Лесниевски-Костарева, Т.А. Дифференциация уголовной ответственности. Теория и законодательная практика / Т.А. Лесниевски-Костарева. – 2-е изд., перераб. и доп. – М.: НОРМА, 2000. – 400 с.

115. Лукинский, И.С., Баулина, А.А. О перспективных направлениях сотрудничества министерства внутренних дел государств – участников СНГ в сфере противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий // Противодействие преступлениям в сфере информационно-телекоммуникационных технологий: сборник научных трудов международной научно-практической конференции. М., 2024. С. 557-561.

116. Ляпунов, Ю.И., Максимов, В.Ю. Ответственность за компьютерные преступления //Законность. 1997. №1. С.8-15.

117. Лебедев, С. Я. Цифровое уголовное право: перспективы формирования и развития (часть 2) / С. Я. Лебедев, В. Ф. Джафарли // Гуманитарные, социально-экономические и общественные науки. – 2024. – № 12. С. 166-170.

118. Мазуров, В.А. Компьютерные преступления: классификация и способы противодействия: учебно-практическое пособие М.: 2002. С.115

119. Мирончик, А.С., Суслопаров, А.В. Хищение в электронной среде как разновидность информационных преступлений: проблемы разграничения и квалификации//Юридические исследования. 2019. № 9. С. 17-30.

120. Мохат, П.М. К вопросу о соответствии автономных интеллектуальных систем вооружений принципам международного гуманитарного права // Вестник военного права 2018. № 2. С. 58–65.

121. Мосечкин, И.Н. Искусственный интеллект и уголовная ответственность: проблемы становления нового вида субъекта преступления // Вестник Санкт-Петербургского университета. 2019. № 3. С. 461–476

122. Наджафи, Г. М. Предмет компьютерных преступлений // Вестник Института законодательства Республики Казахстан, 2012. № 4. С. 125-127.

123. Овчинский, В.С. Криминология цифрового мира: учебник для магистратуры / В. С. Овчинский. — М. : Норма : ИНФРА-М, 2018. — 352 с.

124. Ожегов С.И., Шведова, Н.Ю. Толковый словарь русского языка (А до Я). [Электронный ресурс]. URL: https://ozhegov.info/slovar/?q=%D0%98*.

125. Пелевина, А.В. Общая характеристика преступлений в сфере компьютерной информации. Пробелы в российском законодательстве, 2015. С. 209-211.

126. Плетнева, Д.А. Соотношение обстоятельств, отягчающих уголовную ответственность, и квалифицирующих признаков преступления// Вестник Белорусского государственного университета. 2016. № 4. - С. 101-104.

127. Попов, А. Н. Преступления в сфере компьютерной информации: учебное пособие / А. Н. Попов. — Санкт-Петербург: Санкт-Петербургский юридический институт (филиал) Университета прокуратуры Российской Федерации, 2018. — 68 с.

128. Попов, К.И., Майоров, А.В. «Правовые основы противодействия преступлениям в сфере компьютерной информации в сети Интернет // Вестник УрФО. Безопасность в информационной сфере. 2013. № 3 (9). С. 38–42.

129. Поляков В.В., Лапин С.А. Средства совершения компьютерных преступлений// Доклады ТУСУРа, № 2 (32), 2014. С. 162-166.

130. Противодействие преступлениям, совершаемым в сфере информационных технологий (учебник) (коллектив авторов; под науч. ред. И.А. Калиниченко). – «ИНФРА-М», 2023. - 642 с.

131. Рарог, А.И. (ред.) Уголовное право России. Части общая и особенная. М.: Проспект, 2018. 624 с.

132. Рассолов, И.М. «Киберпреступность: понятие, основные черты, формы проявления». Юридический мир 2, 2008. С44-46.

133. Романов, И.В. Понятие киберпреступлений и его значение для расследования // Сибирские уголовно-процессуальные и криминалистические чтения. 2016. № 5 (13). С. 105-109.

134. Российское уголовное право: в 2 т. Т. 2. Особенная часть / Под ред. Л.В. Иногамовой-Хегай, В.С. Комиссарова, А.И. Рарога. – М.: ТК Велби, Проспект, 2006. 656 с.

135. Россинская, Е.Р. Рядовский И.А. Современные способы компьютерных преступлений и закономерности их реализации. Lex russica. 2019;(3). С. 87-99.

136. Русскевич, В.Е. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ): вопросы квалификации // Уголовное право. 2020. № 5. С. 94 -104.

137. Русскевич, Е.А. Компьютерные преступления: квалификационные алгоритмы и тренды: учебное пособие. М.: Проспект, 2025. 120 с.

138. Савин, А.А., Мешков Д.Н. Субъективная сторона преступления как элемент состава уголовного преступления. // Гуманитарные, социально-экономические и общественные науки. 2021. № 5. С. 148-150.

139. Судакова, Т.М. Принципы интегративного криминологического знания в зарубежной и российской доктринах / Т. М. Судакова // Академический юридический журнал. – 2023. – Т. 24, № 1(91). С. 80-88.

140. Судакова, Т.М. Нейронаука и нейрокриминология: методологические принципы интеграции / Т. М. Судакова // Академический юридический журнал. – 2022. – Т. 23, № 2(88). С. 179-186.

141. Селиванов, Н. А. Проблемы борьбы с компьютерной преступностью / Н.А. Селиванов // Законность. – 1993. – № 8. С.37.

142. Семёнов А.В. Этимологический словарь русского языка. Русский язык от А до Я. М.: ЮНВЕС, 2003. [Электронный ресурс]. URL: https://evartist.narod.ru/text15/001.htm.

143. Уголовное право России. Части Общая и Особенная: учебник (коллектив авторов; под ред. д.ю.н., проф. А.В. Бриллиантова; 3-е изд., перераб. и доп.). – «Проспект», 2021 г. –1344 с

144. Уголовное право Российской Федерации. Общая часть: Учебник для вузов / Под ред. В.С. Комиссарова, Н.Е. Крыловой, И.М. Тяжковой. — М.: Статут, 2012. – 879 с.

145. Уголовное право. Особенная часть: Учебник / Под ред. Л.В. Иногамовой-Хегай, А.И. Рарога, А.И. Чучаева. — 2-е изд., исправл. и доп. — М.: Юридическая фирма «КОНТРАКТ», ИНФРА-М, 2008. – 800 с.

146. Уголовное право Армении и России. Общая и Особенная части (отв. ред. С.С. Аветисян, А.И. Чучаев). – «КОНТРАКТ», 2014 г. [Электронный ресурс]. URL.: https://base.garant.ru/57515102/.

147. Уголовное право. Особенная часть. : учебник / В. В. Бабурин, М. В. Бавсун, И. А. Белецкий [и др.] ; под ред. М. В. Бавсуна. — Москва : КноРус, 2022. — 577 с.

148. Уторова, Т. Н. Преступления в сфере информационной безопасности: учебное пособие / Т. Н. Уторова, Л. А. Колпакова ; Министерство науки и высшего образования Российской Федерации, Московский государственный юридический университет имени О.Е. Кутафина (МГЮА), Северо-Западный институт (филиал) Университета имени О.Е. Кутафина (МГЮА). - Вологда: Северо-Западный ин-т (филиал) Ун-та им. О. Е. Кутафина (МГЮА), 2024.-193 с.

149. Флетчер, Дж., Наумов, А.В. Основные концепции современного уголовного права. М., 1998. – 512 с.

150. Ходусов, А.А. Преступления, совершаемые с использованием информационно-телекоммуникационных средств: философско-правовые конструирование эффективных классификаций//Философия права. 2020. № 3. С. 89-95.

151. Чудинов, С.И. Проблема объективных и субъективных аспектов безопасности // Общество: философия, история, культура. 2015. № 6. С. 47-50.

152. Шахрай, С.С. Объективные и субъективные признаки в обще понятии состава преступлений в сфере компьютерной информации // Вестник Академии экономической безопасности МВД России. № 10. 2010. С. 132-137.

153. Юрченко, И.А. Понятие, классификация и уголовно-правовой статус информации //Сборник материалов к 75 – летию МГЮА. М., 2007. С. 153-164.

154. Юрченко, И.А. Преступления против информационной безопасности: Учебное пособие / И.А. Юрченко — Москва: Проспект, 2021. — 208 с. [Электронный ресурс]. URL: https://book.ru/book/946143.

155. Юрченко, И.А. Преступления против безопасности информации, преступления против информационной безопасности, преступления информационной направленности: определение понятий // УГОЛОВНОЕ

ПРАВО: СТРАТЕГИЯ РАЗВИТИЯ В XXI ВЕКЕ материалы XIV Международной научно-практической конференции. Министерство образования и науки Российской Федерации; Московский государственный юридический университет имени О. Е. Кутафина (МГЮА). Москва, 2017. С. 477-480.

Диссертации, авторефераты и монографии

156. Аминов, И.И. Правовая система Туркмении «генезис и эволюция»: дис. …док.юрид. наук: 5.1.1. - МГИМО, Москва, 2023 – 445 с.

157. Аминов, И.И. Становление и развитие правовой системы Туркменистана: монография / И.И. Аминов. — Москва: РУСАЙНС, 2024. — 378 с.

158. Аминов, И.И. Становление и развитие правовой системы Туркменистана: монография / И. И. Аминов. — Москва: Русайнс, 2024. — 378 с. [Электронный ресурс]. URL: https://book.ru/book/953582 (дата обращения: 13.05.2025).

159. Бегишев, И.Р., Бикеев, И.И. Преступления в сфере обращения цифровой информации: монография. Казань: Изд-во «Познание», 2020. – 300 с

160. Быков, В.М. Преступления в сфере компьютерной информации: криминологические, уголовно-правовые и криминалистические проблемы: монография / В.М. Быков, В.Н. Черкасов. — Москва: Юрлитинформ, 2015. — 325 с.

161. Гаджиев, М.С. Криминологический анализ преступности в сфере компьютерной информации (по материалам республики Дагестан) : Специальность 12.00.08 «Уголовное право и криминология; уголовно-исполнительное право»: автореферат диссертации на соискание ученой степени кандидата юридических наук / Гаджиев Марат Салахетдинович ; Дагестан. гос. ун-т. – Махачкала, 2004. —168 с.

162. Гайфутдинов Р. Р. Понятие и квалификация преступлений против безопасности компьютерной информации: диссертация ... кандидата Юридических наук: 12.00.08 / Гайфутдинов Рамиль Рустамович; [Место защиты: ФГАОУ ВО «Казанский (Приволжский) федеральный университет»], 2017.- 243 с.

163. Ефремова, М.А. Уголовно-правовая охрана информационной безопасности: дисс. … док. юрид. наук: 12.00.08. М. 2017. –427 с.

164. Ефремова, М.А. Уголовно-правовая охрана информационной безопасности: монография. М., 2018. – 312 с.

165. Зуйков, Г.Г. Криминалистическое учение о способе совершения преступления: автореф. дис. … док. юрид. наук. М. : Высш. школа МВД СССР, 1970. – 31 с.

166. Козаев, Н.Ш. Противодействие злоупотреблениям современными технологиями: международно-правовые и уголовно-правовые аспекты: монография / под ред. докт. юрид. наук, проф. А. В. Наумова. - М.: Юрлитинформ, 2016. – 192 с.

167. Крылов, В.В. Основы криминалистической теории расследования преступлений в сфере информации. дис. ... докт. юрид. наук: 12.00.09 / Крылов В.В. - М., 1998. – 334 с.

168. Летелкин, Н.В. Уголовно-правовое противодействие преступление преступлениям, совершаемым с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет»): монография / отв. ред. А.В. Петрянин. – Москва: Проспект, 2021. – 176 с.

169. Овсюков, Д.А. Корыстные преступления против собственности с использованием информационно-телекоммуникационных сетей: вопросы квалификации: Дис. … канд. юрид. наук: 5.1.4/ Д.А. Овсюков. – Москва, 2022. – 231 с.

170. Пучков, Д.В. Уголовно-правовая модель защиты телекоммуникаций от преступных посягательств: проблемы теории и практики: Дис. ... док. юрид. наук : 12.00.08 : Екатеринбург, 2022. – 447 с.

171. Пучков, Д.В. Уголовно-правовая модель защиты телекоммуникаций от преступных посягательств: проблемы теории и практики: Автореф. дисс. … док. юрид. наук: 5.1.4. Е. 2022. – 51 с.

172. Русскевич, Е.А. Уголовное право и «Цифровая преступность»: проблемы и решения: монография. 2-е изд., перераб. и доп. М.: Инфра-М, 2022. – 230 с.

173. Русскевич, Е.А. Дифференциация ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий, и проблемы их квалификации: дисс. ... доктора юридических наук: 12.00.08. М. 2021. – 521 с.

174. Фролов Михаил Дмитриевич. Уголовно-правовое и криминологическое противодействие мошенничеству в сфере компьютерной информации: диссертация ... кандидата Юридических наук: 12.00.08 / Фролов Михаил Дмитриевич; М. 2019. – 211 с.

175. Шахрай, С.С. Система преступлений в сфере компьютерной информации: сравнительно-правовой, социолого-криминологический и уголовно-правовой аспекты: дисс. … кан. юрид. наук: 12.00.08. М. 2010. –214 с.

176. Шипулин, Г.Ф. Предупреждение преступлений, совершаемых с использованием компьютерных сетей дис. канд. юрид. наук. М., 2000. –191 с.

177. Юрченко, И.А. Информация конфиденциального характера как предмет уголовно-правовой охраны: Дис. ... канд. юрид. наук : 12.00.08 : Москва, 2000. – 205 с.

Электронные источники

178. Agari H. Email Fraud Report. 2020. [Электронный ресурс]. URL: https://www.agari.com/cyberintelligence-research/e-books/agari-h22020-email-fraud-report.pdf.

179. В России впервые осудили за непристойное поведение в интернете. [Электронный ресурс]. URL: https://rg.ru/2014/02/19/internet-site.html.

180.Военный энциклопедический словарь. [Электронный ресурс]. URL: https://encyclopedia.mil.ru/encyclopedia/dictionary/list.htm.

181.Игнатова, О., Куликов, В. Кто кого обманывает// Российская газета. 2022. 14 июля. [Электронный ресурс]. URL: www.Rgru.turbopages.ork (дата обращения: 13.08.2023).

182.Бюллетень международных договоров октябрь 2019, № 10, стр. 63-68, Официальный интернет-портал правовой информации. [Электронный ресурс]. URL: (www.pravo.gov.ru) 13.06.2019.

183.Хакеры могли предложить работнику ВГТРК за помощь до $1 млн. [Электронный ресурс]. URL: https://nsn.fm/policy/hakery-mogli-predlozhit-rabotniku-vgtrk-za-pomosch-do-1-mln (дата обращения: 07.10.2024).

184. Суд вынес приговор новосибирскому хакеру за хищение 16 млн руб. [Электронный ресурс]. URL: https://nsk.rbc.ru/nsk/27/10/2023/653b243e9a79474845f748fb.

185. Суд Томска вынес приговор гражданину за использование программы, скрывающей данные пользователя. [Электронный ресурс].URL: https://telesputnik.ru/materials/hipe/news/sud-tomska-vynes-prigovor-grazhdaninu-za-ispolzovanie-programmy-skryvayuschey-dannye-polzovatelya.

186.Челябинца осудили за распространение вредоносных компьютерных программ. [Электронный ресурс]. URL: https://www.kommersant.ru/doc/5902313.

187.Более половины интернет-пользователей столкнулись с кибератаками в 2024 году. [Электронный ресурс]. URL: https://rg.ru/2024/05/27/bolee-poloviny-rossijskih-internet-polzovatelej-stolknulis-s-kiberatakami-v-2024-godu.html (дата обращения: 7.10.2024).

188. Cybercriminals' favourite VPN taken down in global action. [Электронный ресурс]. URL: https://www.europol.europa.eu/newsroom/news/cybercriminals%E2%80%99- favourite-vpn-taken-down-in-global-action.

189. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. [Электронный ресурс]. URL: https://docs.cntd.ru/document/1200058320.

190. Марк Туллий Цицерон Из речи в защиту Клуенция. Legum … servi sumus ut liberi esse possimus. [Электронный ресурс]. URL: https://ru.citaty.net/tsitaty/457359-mark-tullii-tsitseron-my-dolzhny-byt-rabami-zakonov-chtoby-stat-svobodn/.

191. Официальный сайт Международного союза электросвязи. [Электронный ресурс]. URL: https://www.un.org/ru/ecosoc/itu/.

192. Официальный сайт МВД России: состояние преступности. [Электронный ресурс]. URL: ttps://мвд.рф/reports.

193. Самые громкие кибер-атаки на критические инфраструктуры. [Электронный ресурс]. URL: https://habr.com/ru/companies/panda/articles/316500/.

194.Задержаны мошенники, похитившие 421 миллион у пенсионерки из Самары. [Электронный ресурс]. URL: https://rg.ru/2025/02/11/zaderzhany-moshenniki-pohitivshie-421-million-u-pensionerki-iz-samary.html.

195. Прокурор разъясняет (Предусмотрена ли уголовная ответственность за неправомерный доступ к компьютерной информации?). [Электронный

ресурс]. URL: https://epp.genproc.gov.ru/ru/web/proc_73/activity/legaleducation/explain?item=94089592#/.

196. Прокурор разъясняет. Разъяснение понятий совершения преступлений группой лиц, группой лиц по предварительному сговору. [Электронный ресурс]. URL: https://epp.genproc.gov.ru/ru/web/proc_42/activity/legal-education/explain?item=49713816.

197. Рейтинг стран по уровню кибербезопасности. [Электронный ресурс]. URL: https://statistics.securelist.com/ru/ransomware/month.

198.Статистика киберугроз в Туркменистане. [Электронный ресурс]. URL: https://statistics.securelist.com/ru/ransomware/month.

199.Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации, разработанным Генеральной Прокуратурой Российской Федерации от 14.04.2014. [Электронный ресурс]. URL: https://legalacts.ru/doc/metodicheskie-rekomendatsii-po-osushchestvleniiu-prokurorskogo-nadzora-za/.

200. Интернет-пользователь осужден за «эмоциональные» письма в СМИ с домашнего компьютера // Право.ru. [Электронный ресурс]. URL: https://pravo.ru/news/view/59120/ (дата обращения: 12.03.2024).

201.Из выступления Президента Российской Федерации В.В. Путина на конференции «Путешествие в мир искусственного интеллекта» 24.11.2023. [Электронный ресурс]. URL: https://www.1tv.ru/news/20231124/465777vladimir_putin_vystupil_na_plenarnom_zasedanii_konferentsii_posvyaschennoy_iskusstvennomu_intellektu

202.Состояние преступности в Российской Федерации за 2020 год. [Электронный ресурс]. URL: https://xn--b1aew.xn--p1ai/reports/item/22678184/.

203. Состояние преступности в Российской Федерации за 2021 год. [Электронный ресурс]. URL: https://xn--b1aew.xn--p1ai/reports/item/28021552/ (дата обращения: 26.03.2025).
204. Состояние преступности в Российской Федерации за 2022 год. [Электронный ресурс]. URL: https://xn--b1aew.xn--p1ai/reports/item/35396677/.
205. Состояние преступности в Российской Федерации за 2023 год. [Электронный ресурс]. URL: https://xn--b1aew.xn--p1ai/reports/item/47055751/.
206. Состояние преступности в Российской Федерации за 2024 год. [Электронный ресурс]. URL: https://xn--b1aew.xn--p1ai/reports/item/60248328/.
207. Состояние преступности в Туркменистане за 2020-2024 года. [Электронный ресурс]. URL: https://asuda.gov.tm/Default.
208. Цифровизация – ключевой фактор экономического развития. [Электронный ресурс]. URL: https://www.turkmenistan.gov.tm/ru/post/86889/cifrovizaciya-klyuchevoj-faktor-ekonomicheskogo-razvitiya.

Приложение 1

Уважаемые участники!

В рамках осуществления сравнительно-правового исследования на тему «Преступления в сфере компьютерной информации по уголовному законодательству Российской Федерации и Туркменистана: сравнительно-правовое исследование» прошу Вас ответить на важные для исследования вопросы. Ваше мнение является особо важным аспектов при формировании теоретических результатов исследования (Анонимность гарантирована! Результаты опроса будут использованы в обобщённом виде):

Укажите Вашу сферу деятельности _____ (адвокат, работник правоохранительных органов, работник судебных органов и т.д.).

1. Согласны ли вы с утверждением, что по своей правовой природе «компьютерные» преступления являются многообъектными общественно опасными посягательствами?

- да; (95,8 %)
- нет, утверждение является неверным; (2,8 %)
- другое. (1,4%)

2. Какое из понятий, по вашему мнению, шире по смыслу: «преступления в сфере информатики и связи» либо «преступления против компьютерной информации»?

- преступления в сфере информатики и связи; (84,5%)
- преступления в сфере компьютерной информации; (12,7 %)
- другое. (2,8 %)

3. На ваш взгляд, что является предметом преступлений в сфере компьютерной информации?

- компьютерная информация и национальная критическая информационная инфраструктура; (70,4%)

- информационно-телекоммуникационные сети; (2,8 %)

- средства хранения информации (USB-флешки, облачные хранилища, карты памяти и т.д); (16,9 %)

- материальные блага (вещи, деньги, имущество, документы); (9,9%)

- преступления в сфере компьютерной информации следует считать беспредметными;

- другое.

4. С вашей точки зрения, что является средством совершения преступлений в сфере компьютерной информации?

- компьютерные устройства (компьютеры, ноутбуки, флеш-карты, планшеты, смартфоны, жесткие диски); (4,2%)

- программное обеспечение; (1,4 %)

- информационно-телекоммуникационные сети;

- компьютерные устройства (компьютеры, ноутбуки, флеш-карты, планшеты, смартфоны, жесткие диски); программное обеспечение; информационно-телекоммуникационные сети; (88,7 %)

- другое. (5,7%)

5. По вашему мнению, что следует считать местом совершения «компьютерных» преступлений?

- место наступления последствий, входящих в объективную сторону преступлений; (64,8%)

- место выполнения лицом действий, входящих в объективную сторону преступлений; (32,4%)

- другое. (2,8 %)

6. Согласны ли вы с утверждением, что термин «киберпреступность» по своей природе является криминологической, а не уголовно-правовой категорией?

- да; (97,2 %)

- нет; (2,8 %)

- другое.

7. Отличаются ли преступления в сфере компьютерной информации своеобразием мотивации и целенаправленности?

- да; (63,4 %)

- нет; (33,8 %)

- другое. (2,8%)

8. Субъекта преступлений в сфере компьютерной информации следует характеризовать как:

- вменяемое физическое лицо, достигшее 16-летнего возраста; (26,8%)

- лицо, пользователь компьютерного устройства, злоупотребивший своим служебным положением; (11,3%)

- лицо, обладающее знаниями в сфере информатики; (5,6%)

- вменяемое физическое лицо, достигшее 16-летнего возраста, злоупотребивший своим служебным положением, лицо, обладающее знаниями в сфере информатики. (56,3%).

9. Как вы считаете, целесообразно ли предусматривать рецидив как квалифицирующий признак преступлений в сфере компьютерной информации?

- да; (38 %)
- нет; (59,2%)
- другое. (2,8%)

С уважением,
аспирант кафедры уголовного
права и криминологии
Корпеев Ата Гельдыевич

Приложение 2

САМАРСКИЙ УНИВЕРСИТЕТ
SAMARA UNIVERSITY

федеральное государственное автономное
образовательное учреждение высшего образования
«Самарский национальный исследовательский университет
имени академика С.П. Королева»

ул. Московское шоссе, д. 34, г. Самара, 443086
Тел.: +7 (846) 335-18-26 , факс: +7 (846) 335-18-36
Сайт: www.ssau.ru, e-mail: ssau@ssau.ru
ОКПО 02068410, ОГРН 1026301168310,
ИНН 6316000632, КПП 631601001

03 ФЕВ 2025 № 235-433

На №_____ от_____

Председателю
Верховного Суда Туркменистана

Б.Г. Ходжамгулыеву

Туркменистан, г. Ашахабад,
ул. Алишера Навои, д. 86

Глубокоуважаемый Бегенч Гурбангелдиевич!

Корпеевым Ата Гельдыевичем, помощником ректора, ассистентом кафедры теории и истории государства и права и международного права юридического института федерального государственного автономного образовательного учреждения высшего образования «Самарский национальный исследовательский университет имени академика С.П. Королева» в рамках диссертационного исследования на тему: «Преступления в сфере компьютерной информации по уголовному законодательству Российской Федерации и Туркменистана: сравнительно-правовое исследование» разработан проект постановления Пленума Верховного Суда Туркменистана «О некоторых вопросах, возникающих у судов при рассмотрении уголовных дел о преступлениях в сфере компьютерной информации» (далее – проект постановления). Позвольте представить Вам проект постановления для ознакомления и возможного использования в работе.

Будем благодарны Вам за обратную связь (тел.: +79631157171, email: atakor@mail.ru, почтовый адрес: 443086, Российская Федерация, г. Самара, ул. Гая, д. 38 А).

Пользуясь случаем просим принять уверение в высоком уважении к Вам и готовности к продолжению плодотворного сотрудничества.

Приложение: Проект постановления на 6 л.

С уважением,

Директор
юридического института
Самарского университета
Заслуженный юрист
Российской Федерации,
доктор юридических наук,
профессор

А.Г. Безверхов

Проект постановления Пленума Верховного Суда Туркменистана «О некоторых вопросах, возникающих у судов при рассмотрении уголовных дел о преступлениях в сфере компьютерной информации»

Для формирования единых подходов, обеспечивающих всестороннее и справедливое разрешение судами вопросов, возникающих при применении уголовного законодательства, предусматривающего ответственность за преступления в сфере компьютерной информации (раздел XXXIII «Преступления против информатики и связи»), Пленум Верховного Суда Туркменистана, руководствуясь п. 3 статьи 38 Закона Туркменистана от 15 августа 2009 года № 49-IV «О суде», постановляет.

1. Судам следует обратить внимание, что объективные признаки преступлений, предусмотренных разделом XXXIII «Преступления против информатики и связи», имеют бланкетный характер, в связи с этим при рассмотрении уголовных дел о преступлениях, предусмотренных разделом XXXIII «Преступления против информатики и связи», судам следует руководствоваться положениями действующего законодательства Туркменистана, регламентирующего вопросы применения информационных технологий, обеспечения информационной безопасности, регулирования развития сети «Интернет» и оказания услуг в сети «Интернет», в частности Законом Туркменистана от 3 мая 2014 года № 72-V «Об информации и ее защите», Законом Туркменистана от 20.12.2014 № 159-V «О правовом регулировании развития сети «Интернет» и оказания интернет услуг», а также иными нормативными правовыми актами (законы, подзаконные акты), международными договорами (соглашениями), ратифицированными Туркменистаном, в области противодействия преступлениям в сфере компьютерной информации, обеспечения безопасности в сфере применения информационных технологий, а также обеспечения информационной безопасности, в частности Соглашением между Правительством Российской

Федерации и Правительством Туркменистана о сотрудничестве в области обеспечения международной информационной безопасности (заключено 5 апреля 2019 года в городе Москва).

2. Исходя из объективной стороны составов преступлений, предусмотренных статьями 373, 374, 375, 377 УК Туркменистана, под компьютерной информацией понимается электронная информация (имеющая вид текстового, числового, звукового и графического содержания), представленная в символьной форме, содержащаяся на материальных электронно-вычислительных носителях, а также различных информационно-телекоммуникационных сетях связи.

Электронно-вычислительными носителями являются устройства, предназначенные для автоматической обработки и передачи информации, в том числе персональные компьютеры, промышленные компьютеры, смартфоны, портативные игровые приставки, суперкомпьютеры; носители информации в форме полупроводниковых устройств, в том числе флеш-карты, диски s sd; оптические устройства, в том числе диски DVD, CD, Blu-ray; магнитные устройства, в том числе жесткие диски, дискеты, а также иные информационные устройства.

3. В соответствии со статями 373, 374, 375, 377, 379, 380 УК Туркменистана под охраняемой законом информацией следует понимать сведения, для которых установлен особый статус правовой защиты действующим законодательством Туркменистана. Вместе с тем особый статус правовой защиты такой информации предусматривает специальные правила ее хранения, обработки и распространения в целях обеспечения ее конфиденциальности.

При этом к информации с особым статусом правовой защиты могут относиться любые сведения, подпадающие под действие законодательства Туркменистана, регулирующего отношения, связанные с государственной, корпоративной, семейной, личной тайной.

4. В статьях раздела XXXIII «Преступления против информатики и связи» следует понимать:

под информационной сетью - совокупность компьютерных устройств, объединенных между собой каналами связи для передачи компьютерной информации;

под копированием информации – создание дубликата данных (информации) путем их электронного перемещения с головного электронно-вычислительного устройства на второстепенные электронно-вычислительные устройства, а также путем воспроизведения дубликата данных в материальной форме (к таким относятся фотографирование, перенос информации на бумажный носитель рукописным способом, воспроизведение информации на иных технических устройствах).

под нарушением нормальной работы информационной системы и информационно-телекоммуникационной сети – постороннее вмешательство в деятельность объектов системы информационного обеспечения и информационных сетей, а равно критическую информационную инфраструктуру.

При этом к внештатным ситуациям следует относить умышленное проникновение в информационную систему или каналы связи с помощью информационных технологий, в том числе программного обеспечения, со стороны лиц, не имеющих права разрешительного доступа, предусмотренного регламентом работы информационной системы и сетей связи, нормативными правовыми актами, техническими документами в сфере информационной безопасности, а также совершение действий, повлекших нарушение целостности сведений, содержащихся в информационной системе и каналах связи.

под изменением идентификационного кода абонентского устройства – незаконное умышленное, без права доступа, изменение кода абонентского устройства (мобильные телефоны, стационарные телефоны, устройства

громкой связи), присваиваемого изготовителем данного устройства, и передающегося оператору связи при подключении устройства к нему.

5. По смыслу статьи 375 УК Туркменистана преступление следует считать оконченным в случае наступления хотя бы одного последствия, указанного в ч.1 ст. 375 УК Туркменистана, а именно умышленного уничтожения либо изменения формата охраняемой законом информации.

6. Судам обратить внимание, что согласно ч.1 ст. 379 УК Туркменистана под преднамеренным использованием или распространением вредоносной программы следует понимать незаконное умышленное внедрение в информационную систему либо иные информационные технологии вредоносной программы, разработанной намеренно для предоставления доступа к ней определенному или неопределённому кругу лиц путем использования различных объектов и каналов распространения (в том числе файлы корпоративных документов, передача сообщений через электронный почтовый ящик, социальные сети, мессенджеры (фишинговые сообщения), установка драйвером операционной системы, сеть «Интернет», использование зараженного USB–порта, флеш-карты, компрометация легитимных программ), с целью уничтожения, изменения компьютерной информации, нарушения естественной работы компьютерного устройства, включая средства его защиты, а также иных информационных технологий.

При этом моментом окончания преступления, предусмотренного ч.1 статьи 379 УК Туркменистана, следует считать создание сегмента машинного кода вредоносной программы, позволяющего осуществить незаконный доступ к охраняемой законом информации. Вместе с тем в случае установления факта создания сегмента машинного кода вредоносной программы данное действие следует квалифицировать как создание вредоносной программы.

7. Под тяжкими последствиями (квалифицирующий признак) в статьях 373-379 УК Туркменистана следует понимать длительную приостановку функционирования национальной электронной системы, информационной

системы критически важных государственных предприятий, иных предприятий любой формы собственности, правовая защита которых установлена действующим законодательством Туркменистана.

8. При квалификации действий лица по ч.1 статьи 380 УК Туркменистана судам необходимо определить путем применения действующего законодательства Туркменистана, является ли распространённая информация ограниченной либо запрещенной к распространению.

По смыслу ч.1 статьи 380 УК Туркменистана владельцем информации является лицо, которому принадлежит информация, а также право распоряжения ею; владеющим лицом является субъект, имеющий полномочия для распоряжения такой информацией в пределах установленных прав.

При этом лицо, имеющее полномочия для распоряжения информацией с разрешительным ограничением, должно быть надлежащим образом ознакомлено с нормативными правовыми актами, локальными нормативными актами либо иными распорядительными документами о таких разрешительных ограничениях до наделения полномочиями.

9. Обратить внимание судов, что действия преступления, предусмотренного ст. 381 УК Туркменистана, образующие объективную сторону, могут повлечь за собой наступление общественно опасных последствий, предусмотренных иными статьями Особенной части УК Туркменистана. В таком случае подобные действия следует рассматривать по совокупности преступлений.

При квалификации преступления, предусмотренного ст. 381 УК Туркменистана, под размещением интернет-ресурсов, преследующих незаконные цели, следует понимать размещение информации в виде рекламно-информационных материалов в информационной системе, имеющей постоянный доступ к сети «Интернет», нарушающих требования действующего законодательства Туркменистана, в том числе содержащих

признаки составов преступлений, предусмотренных уголовным законодательством Туркменистана.

Под лицом, оказывающим услуги по размещению интернет-ресурсов, следует понимать физическое лицо (поставщика), предоставляющее комплекс технических услуг в сфере информационных технологий по размещения сведений (информации) в информационно-телекоммуникационных сетях, в том числе сети «Интернет».

10. При квалификации преступления, предусмотренного ч.1 ст. 383 УК Туркменистана, судам следует установить, действительно ли лицом были увеличены технические возможности беспилотных летающих аппаратов (далее – БПЛА), заявленные в технической документации производителя БПЛА, а также в сертификате летной годности БПЛА. В случае установления факта изменения технических возможностей БПЛА, следует установить, проведена ли повторная сертификация технических изменений БПЛА.