Федеральное государственное автономное образовательное учреждение высшего образования «Московский государственный юридический университет имени О.Е. Кутафина (МГЮА)»

На правах рукописи

Вострова Алеся Николаевна

УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ ЗА СОЗДАНИЕ, ИСПОЛЬЗОВАНИЕ И РАСПРОСТРАНЕНИЕ ВРЕДОНОСНЫХ КОМПЬЮТЕРНЫХ ПРОГРАММ ПО ЗАКОНОДАТЕЛЬСТВУ РОССИЙСКОЙ ФЕДЕРАЦИИ И КЫРГЫЗСКОЙ РЕСПУБЛИКИ: СРАВНИТЕЛЬНО-ПРАВОВОЕ ИССЛЕДОВАНИЕ

Специальность 5.1.4. Уголовно-правовые науки

Диссертация
на соискание ученой степени
кандидата юридических наук

Научный руководитель:
доктор юридических наук, доцент
Русскевич Евгений Александрович

Москва – 2026

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ.....4

Глава 1. УГОЛОВНО-ПРАВОВОЕ ПРОТИВОДЕЙСТВИЕ СОЗДАНИЮ, ИСПОЛЬЗОВАНИЮ И РАСПРОСТРАНЕНИЮ ВРЕДОНОСНЫХ КОМПЬЮТЕРНЫХ ПРОГРАММ: ОБЩЕТЕОРЕТИЧЕСКИЙ АНАЛИЗ.....19

§ 1. Состояние и основные направления противодействия киберпреступности в Российской Федерации и Кыргызской Республике.....19

§ 2. Международный опыт противодействия киберпреступности.....37

§ 3. Ответственность за действия с вредоносными компьютерными программами по законодательству стран Содружества Независимых Государств…….....57

Глава 2. УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА СОЗДАНИЯ, ИСПОЛЬЗОВАНИЯ И РАСПРОСТРАНЕНИЯ ВРЕДОНОСНЫХ КОМПЬЮТЕРНЫХ ПРОГРАММ ПО ЗАКОНОДАТЕЛЬСТВУ РОССИЙСКОЙ ФЕДЕРАЦИИ И КЫРГЫЗСКОЙ РЕСПУБЛИКИ.....75

§ 1. Объект создания, использования и распространения вредоносных компьютерных программ (ст. 273 УК РФ, ст. 320 УК КР)……75

§ 2. Объективная сторона создания, использования и распространения вредоносных компьютерных программ (ст. 273 УК РФ, ст. 320 УК КР.....99

§ 3. Субъективные признаки создания, использования и распространения вредоносных компьютерных программ (ст. 273 УК РФ, ст. 320 УК КР).....115

ГЛАВА 3. ПЕРСПЕКТИВНЫЕ НАПРАВЛЕНИЯ СОВЕРШЕНСТВОВАНИЯ ЗАКОНОДАТЕЛЬСТВА И ПРОБЛЕМЫ КВАЛИФИКАЦИИ СОЗДАНИЯ, ИСПОЛЬЗОВАНИЯ И РАСПРОСТРАНЕНИЯ ВРЕДОНОСНЫХ КОМПЬЮТЕРНЫХ ПРОГРАММ.....128

§ 1. Особенности и проблемы квалификации создания, использования и распространения вредоносных компьютерных программ……..……128

§ 2. Основные направления совершенствования уголовного законодательства Российской Федерации и Кыргызской Республики об ответственности за создание, использование и распространение вредоносных компьютерных программ.....146
ЗАКЛЮЧЕНИЕ.....163
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ.....167
ПРИЛОЖЕНИЕ № 1 191
ПРИЛОЖЕНИЕ № 2 197
ПРИЛОЖЕНИЕ № 3 198

ВВЕДЕНИЕ

Актуальность темы диссертационного исследования. Современный эволюционный этап технологического развития характеризуется всеобъемлющей цифровизацией. Критерий «оцифрованность» стал в некотором роде мерилом оценки развитости в экономике, государственном управлении и во многих иных сферах (образование, медицина и др.). При этом человечество столкнулось с новым пониманием «вредоносности» информации, которая проявляется не в идеологическом, эстетическом или ином информационном воздействии на человека (террористическая пропаганда, порнография и проч.), а в способности деструктивного воздействия на саму информацию.

Считается, что исторически первый по-настоящему масштабный инцидент безопасности с использованием вредоносного компьютерного кода произошел в 1986 г., когда пакистанские программисты братья Базит и Амжат Фарук Альви создали вирус «Brain» – первый известный в мире компьютерный вирус, заражавший персональные компьютеры пользователей под управлением операционной системы MS-DOS. Благие намерения разработчиков вредоносной программы – они ссылались на то, что действовали из соображений защиты авторского права медицинского программного обеспечения – привели к заражению компьютеров сотен тысяч пользователей по всему миру[1]. С этого момента принято вести своего рода отсчет эволюции вредоносных программ, которые в настоящее время уже представляют собой сложные многофункциональные программные продукты, используемые как преступными группами, так и отдельными государственными структурами в целях кибершпионажа и иной подрывной (диверсионной) деятельности. Последние массовые компьютерные атаки, совершенные с использованием вредоносных программ (WannaCry, Petya и др.), показали их огромную разрушительную силу в условиях, когда многие развитые и

[1] См.: *Philip Elmer-Dewitt (26 сентября 1988 г.)*. URL: https://time.com/archive/6713325/technology-you-must-be-punished/ (дата обращения: 09.01.2025).

развивающиеся страны делают ставку на инновационное технологическое развитие и построение цифровой экономики.

Ответом на эти вызовы во многих странах стало формирование специального механизма уголовно-правовой охраны, направленного на криминализацию и, соответственно, последующую квалификацию подобных деяний как преступных.

Предсказуемо, что в этом вопросе уголовное законодательство Российской Федерации и Кыргызской Республики как правопреемников общего советского юридического наследия, развивающееся в условиях тесного взаимодействия в рамках евразийского интеграционного пространства, демонстрируют в целом схожие подходы. Хотя уже можно указать и на то, что за последнее десятилетие наметились и вполне существенные различия в регламентации ответственности за преступления в сфере компьютерной информации, в том числе в части ответственности за действия с компьютерными вредоносными программами.

Большинство информационных способов модернизации могут иметь скрытый «враждебный потенциал», который может быть направлен против безопасности самого общества[2]. Опасность компьютерных преступлений признают многие. Так, Президент Кыргызской Республики С. Н. Жапаров в своем выступлении, приуроченном к открытию специального центра по обеспечению кибербезопасности, особо подчеркнул, что обеспечение кибербезопасности цифровых инфраструктур и сервисов, которые активно создаются в Кыргызстане, является одним из важнейших аспектов противостояния вызовам современности[3].

Анализ тенденций в сфере изменения уголовного законодательства выявляет нарастающую криминализацию посягательств в сфере компьютерной информации, ужесточение ответственности за преступления, совершаемые с использованием IT-инструментов, а также поиск оптимальных правовых решений для противодействия новым угрозам, включая неправомерное воздействие на

---

[2] См.: Сейдакматов Н.А. Правовое обеспечение информационной безопасности // Вестник КРСУ. 2024. Т. 24. № 3. С. 101–106.

[3] См.: Открытие Центра по обеспечению кибербезопасности. URL: https://ru.sputnik.kg/20230513/kyrgyzstan-kiberbezopasnost-zdanie-centr-gknb1075288960.html (дата обращения: 10.02.2026).

критическую инфраструктуру[4]. Вместе с тем применительно к Кыргызстану, несмотря на проводимые реформы, можно согласиться с тем, что «отсутствует единая устойчивая государственная уголовная политика в стране», что приводит к фрагментарности правового регулирования и законодательным «качелям» между гуманизацией и ужесточением репрессий[5].

Все это, думается, актуализирует проведение сравнительно-правовых исследований, направленных на анализ прежде всего имеющегося российского опыта как более устоявшейся модели уголовно-правовой охраны, способной выступить своего рода ориентиром для совершенствования законодательства в Кыргызской Республике.

По данным Главного информационно-аналитического центра Министерства внутренних дел Российской Федерации в 2021 г. совершено 517,7 тыс. 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», а преступлений в сфере компьютерной информации зарегистрировано 6869[6]. В 2022 г. зарегистрировано 522,1 тыс. таких преступлений, что на 0,8% больше, чем за аналогичный период прошлого года, при этом 381,1 тыс. (73%) совершены с использованием сети «Интернет», а количество преступлений в сфере компьютерной информации возросло до 10 027[7]. В 2023 г. зарегистрировано 677,0 тыс. преступлений, что на 29,7% больше, чем за аналогичный период прошлого года, при этом 526,8 тыс. (77,8%) совершены с использованием сети «Интернет», а преступлений в сфере компьютерной информации зарегистрировано

---

[4] См.: Щепельков В.Ф. Перспективы уголовно-правового противодействия компьютерным преступлениям // Вестник Волгоградской академии МВД России. 2024. № 3 (70). С. 9–14.

[5] См.: Сыдыкова Л.Ч. Проблемы и пути развития современной уголовной политики в Кыргызстане // Вестник КРСУ. 2025. Т. 25. № 11. С. 113–120.

[6] См.: Состояние преступности в Российской Федерации за январь – декабрь 2021 года. [Электронный ресурс]. URL: https://xn--b1aew.xn--p1ai/reports/item/28021552/ (дата обращения: 25.02.2026).

[7] См.: Состояние преступности в Российской Федерации за январь – декабрь 2022 года. [Электронный ресурс]. URL: https://xn--b1aew.xn--p1ai/reports/item/35396677/ (дата обращения: 25.02.2026)

37 101[8]. В 2024 г. зарегистрировано 765,4 тыс. преступлений, что на 13,1% больше, чем за аналогичный период прошлого года, при этом 649,1 тыс. (84,8%) совершены с использованием сети «Интернет», а преступлений в сфере компьютерной информации зарегистрировано 105 773[9]. В 2025 г. зарегистрировано 675,4 тыс. таких преступлений, что на 11,8% меньше, чем за аналогичный период прошлого года, при этом количество преступлений в сфере компьютерной информации составило 61 137[10].

В Кыргызской Республике, согласно статистическим данным, опубликованным на официальном сайте Верховного суда Кыргызской Республики в разделе отчетности о рассмотрении уголовных дел судами первой инстанции, наблюдается следующая динамика по ст. 320 Уголовного кодекса Кыргызской Республики (далее – УК КР). В статистических сводках за 2021 г. какая-либо информация по данной категории дел отсутствует. За 2022 г. количество рассмотренных дел по указанной статье составило 0, аналогичный нулевой показатель зафиксирован и по итогам 2023 г. В 2024 г. в остатке неоконченных дел на начало отчетного периода числилось два дела, в течение года дополнительно поступило три дела, из которых: одно дело было рассмотрено с вынесением обвинительного приговора, производство по одному делу было прекращено, и еще одно дело было передано по подсудности в другой суд[11]. Таким образом, остаток нерассмотренных дел на конец 2024 г. составил два дела. За девять месяцев 2025 г. в производство судов поступило одно дело, которое было рассмотрено по существу

---

[8] См.: Состояние преступности в Российской Федерации за январь – декабрь 2023 года. [Электронный ресурс]. URL: https://xn--b1aew.xn--p1ai/reports/item/47055751/ (дата обращения: 25.02.2026).

[9] См.: Состояние преступности в Российской Федерации за январь – декабрь 2024 года. [Электронный ресурс]. URL: https://xn--b1aew.xn--p1ai/reports/item/60248328/ (дата обращения: 25.02.2026).

[10] См.: Состояние преступности в Российской Федерации за январь – декабрь 2025 года. [Электронный ресурс]. URL: https://xn--b1aew.xn--p1ai/reports/item/77848182/ (дата обращения: 25.02.2026).

[11] См.: Отчет о работе судов первой инстанции по рассмотрению уголовных дел за 2021-2024 гг. [Электронный ресурс]. URL: https://sot.kg/statistics/main/index.php (дата обращения: 15.04.2026).

с вынесением приговора[12]. Следует отметить, что приведенные сведения о рассмотрении уголовных дел по ст. 320 УК КР являются единственной официально открытой статистикой, связанной с данной категорией преступлений. Подобная динамика характеризуется практически нулевыми показателями. И это при том, что страна, равно как и Россия в настоящее время, переживает этап активной цифровой модернизации государственного управления, экономики и всей общественной жизни. Думается, что причины такого положения, конечно же, заключаются не в отсутствии самой практики совершения посягательств на отношения в сфере цифровой безопасности, а в том, что зачастую именуется «селективностью» или избирательностью уголовной репрессии. Символичность положений кыргызского уголовного законодательства об ответственности за действия, связанные с вредоносными компьютерными программами, имеет свои корни в восприятии данной проблемы населением и на уровне правоприменения, в отсутствии наработанных методик раскрытия и расследования подобных преступлений, а также в том, что судебная практика не имеет конкретных рекомендаций по применению ст. 320 УК КР (хотя, безусловно, это можно распространить на все компьютерные преступления по законодательству Кыргызстана). И в этом отношении Российская Федерация опережает Кыргызстан в накопленном опыте, изученности и понимании природы, содержания и опасности посягательств с использованием вредоносных компьютерных программ.

Кроме актуальности собственно сравнительно-правового аспекта, важно указать и на то, что как в российской теории уголовного права, так и в немногочисленной доктрине Кыргызстана имеется множество нерешенных вопросов, связанных с пониманием отдельных признаков преступлений в сфере оборота вредоносных компьютерных программ. Из многих имеющихся подходов нельзя составить общепринятого понимания даже относительно определения ключевого признака вредоносности компьютерной программы или информации.

---

[12] См.: Статистические данные по уголовным делам, рассмотренным судами первой инстанции за 9 месяцев 2025 года. [Электронный ресурс]. URL: https://sot.kg/statistics/main/index.php (дата обращения: 15.04.2026).

Однако остропроблемный характер имеют многие другие вопросы, возникающие, например, на стыке основных институтов Общей части уголовного права: квалификация соучастия при использовании вредоносных программ, квалификация множественности при распространении и (или) использовании одного и того же экземпляра или нескольких экземпляров вредоносных компьютерных программ и др.

Таким образом, специальное сравнительно-правовое исследование уголовной ответственности за преступления, связанные с оборотом вредоносных компьютерных программ, по законодательству Российской Федерации и Кыргызской Республики является востребованным в современных условиях, обладает выраженной теоретической и практической значимостью.

Степень научной разработанности темы исследования. Теоретическую основу настоящего диссертационного исследования составляют труды специалистов в области уголовного права, криминологии и информационной безопасности. В Российской Федерации значительный вклад в разработку общих вопросов уголовной политики и квалификации преступлений внесли М.М. Бабаев, Ю.В. Грачева, И.Э. Звечаровский, Л.В. Иногамова-Хегай, Н.Г. Кадников, А.И. Коробеев, В.Н. Кудрявцев, Н.Ф. Кузнецова, Н.А. Лопашенко, А.В. Наумов, К.В. Ображиев, Н.И. Пикуров, Ю.Е. Пудовочкин, А.И. Рарог, А.И. Чучаев, П.С. Яни, Б.В. Яцеленко и др.

В Кыргызской Республике формирование теоретической основы уголовного права нашло отражение в работах К.Ш. Курманова, К.М. Осмоналиева, Л.Ч. Сыдыковой и Т.А. Асаналиева.

Фундаментальные аспекты уголовно-правовой охраны информационной безопасности и противодействия компьютерной преступности нашли отражение в диссертационных исследованиях: В.Б. Вехова «Криминалистическая характеристика и совершенствование практики расследования и предупреждения преступлений, совершаемых с использованием средств компьютерной техники» (1995 г.), В.Г. Степанова-Егиянца «Методологическое и законодательное обеспечение безопасности компьютерной информации в Российской Федерации:

уголовно-правовой аспект» (2016 г.), М.А. Ефремовой «Уголовно-правовая охрана информационной безопасности» (2018 г.), Е.А. Русскевича «Дифференциация ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий, и проблемы их квалификации» (2021 г.), К.Н. Евдокимова «Противодействие компьютерной преступности: теория, законодательство, практика» (2022 г.), Д.В. Пучкова «Уголовно-правовая модель защиты телекоммуникаций от преступных посягательств: проблемы теории и практики» (2022 г.), И.Р. Бегишева «Уголовно-правовая охрана общественных отношений, связанных с робототехникой» (2022 г.), В.Ф. Джафарли «Формирование и развитие системы криминологической безопасности в сфере информационно-коммуникационных технологий» (2022 г.).

Непосредственно вопросам, связанным с установлением и реализацией уголовной ответственности за оборот вредоносных компьютерных программ, посвящены работы В.Ю. Максимова «Незаконное обращение с вредоносными программами для ЭВМ: проблемы криминализации, дифференциации ответственности и индивидуализации наказания» (1998 г.), Л.Н. Соловьева «Расследование преступлений, связанных с созданием, использованием и распространением вредоносных программ для ЭВМ» (2003 г.), М.М. Малыковцева «Уголовная ответственность за создание, использование и распространение вредоносных программ для ЭВМ» (2006 г.).

При этом важно отметить, что последнее диссертационное исследование, непосредственно посвященное проблематике незаконного оборота вредоносных компьютерных программ, было проведено в 2008 г. Е.А. Маслаковой «Незаконный оборот вредоносных компьютерных программ: уголовно-правовые и криминологические аспекты».

В Кыргызской Республике отсутствуют комплексные монографические исследования, специально посвященные уголовно-правовым аспектам противодействия обороту вредоносных компьютерных программ.

Самостоятельное сравнительно-правовое исследование уголовной ответственности за преступления, связанные с оборотом вредоносных

компьютерных программ, по законодательству Российской Федерации и Кыргызской Республики ранее также не проводилось.

Объектом исследования выступают общественные отношения, возникающие в связи и по поводу установления и реализации уголовной ответственности за создание, использование и распространение вредоносных компьютерных программ по уголовному законодательству Российской Федерации и Кыргызской Республики.

Предметом исследования являются социально-экономические, технологические и политические предпосылки криминализации, состояние, закономерности и ключевые особенности законодательного определения и реализации ответственности за действия в сфере незаконного оборота вредоносных компьютерных программ в Российской Федерации и Кыргызской Республике.

Цель исследования заключается в проведении комплексного анализа уголовного законодательства, предусматривающего ответственность за создание, использование и распространение вредоносных компьютерных программ в Российской Федерации и Кыргызской Республике, получении на этой основе нового теоретического знания, способствующего общему развитию учения об уголовной ответственности за киберпреступления.

Для достижения поставленной цели были определены и последовательно решены следующие **задачи** исследования:

- проанализированы состояние и тенденции уголовной политики противодействия киберпреступности в Российской Федерации и Кыргызской Республике;

- исследованы международные договоры и иные документы, определяющие критерии криминализации ответственности за преступления, связанные с вредоносными компьютерными программами;

- выделены и изучены социально-экономические предпосылки криминализации действий с вредоносными компьютерными программами;

- осуществлен анализ зарубежного уголовного законодательства (выборочно) в части выявления основных тенденций в области уголовно-правового противодействия действиям с вредоносными компьютерными программами;

- проведен комплексный сравнительно-правовой анализ уголовно-правовых норм, предусматривающих ответственность за создание, использование и распространение вредоносных компьютерных программ, по законодательству Российской Федерации и Кыргызской Республики;

- проанализирован и уточнен категориальный аппарат в исследуемой сфере;

- определены особенности и выделены проблемы квалификации преступлений, предусмотренных ст. 273 УК РФ и ст. 320 УК КР;

- разработаны научно обоснованные предложения по совершенствованию законодательства об ответственности за преступления, предусмотренные ст. 273 УК РФ и ст. 320 УК КР.

Методологическую основу диссертационного исследования составила совокупность общенаучных и частнонаучных методов познания, применение которых позволило обеспечить достоверность и обоснованность полученных выводов и положений.

Использование историко-правового метода дало возможность проследить эволюцию уголовного законодательства обоих государств в сфере противодействия компьютерной преступности, выявить факторы, повлиявшие на его развитие, и оценить эффективность предшествующих правовых моделей.

Фундаментальное значение имел сравнительно-правовой метод, который позволил провести сопоставительный анализ уголовного законодательства Российской Федерации и Кыргызской Республики, выявить общие черты и различия в подходах к криминализации деяний, связанных с вредоносными программами, в определении их признаков, а также в регламентации ответственности за их совершение.

Формально-юридический метод применялся при анализе содержания уголовно-правовых норм, установлении их логических связей, толковании терминов и понятий, используемых в законодательстве. Метод правового

моделирования использовался при разработке предложений по совершенствованию уголовного законодательства и практики его применения.

Совокупность примененных методов исследования обеспечила комплексный и всесторонний характер изучения проблемы, достоверность и обоснованность сформулированных в диссертации выводов и предложений.

Научная новизна диссертации во многом определяется самой постановкой цели и исследовательских задач. Работа представляет собой первое в юридической науке Российской Федерации и Республики Кыргызстан комплексное сравнительно-правовое исследование уголовной ответственности за создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ и ст. 320 УК КР). Полученные теоретические выводы дополняют и развивают доктрину двух стран об уголовной ответственности за компьютерные преступления в целом. Научная новизна работы также определяется уточнением категориального аппарата по исследуемой теме, а также формулированием оригинальных предложений по совершенствованию законодательства и правоприменения.

Научная новизна диссертации во многом определяется **положениями, выносимыми на защиту:**

1. Выделение вредоносной компьютерной программы и (или) информации в качестве предмета преступления отражает тот факт, что этот предмет сам по себе создает угрозу для отношений в сфере общественной безопасности. Однако в отличие от схожих уголовно-правовых запретов, например в сфере оборота оружия и наркотических средств, нормам об ответственности за действия с вредоносными компьютерными программами характерна значительно большая правовая неопределенность (по причине отсутствия «размерных» признаков предмета преступления, тяжести наступивших последствий, специальных мотивов и (или) целей деяния и т.п.).

2. Эволюция криминообразующего признака «вредоносная компьютерная программа» в уголовном законодательстве России и Кыргызстана прошла принципиально разные пути. Если российское законодательство, впервые

закрепив его в УК РФ 1996 г., в дальнейшем развивалось посредством его использования в новых уголовно-правовых запретах (ст. 138^1, 274^1 УК РФ), сохраняя при этом понятийную преемственность, то в Кыргызстане наблюдалась терминологическая нестабильность. Смена трех уголовных кодексов (1997, 2017, 2021 гг.) привела к трансформации признака от «вредоносных программ для ЭВМ» до «вредоносных компьютерных программ», а немногим позднее уже к «вредоносным программным продуктам», что свидетельствует об отсутствии устоявшейся доктринальной и законодательной концепции в данной сфере.

3. В российском уголовном законе нормы об ответственности за действия с вредоносными компьютерными программами рассредоточены сразу по нескольким статьям (ст. 273, 274^1 УК РФ), а смежный запрет затрагивается в ст. 138^1 УК РФ. В то же время кыргызский подход остался консервативным и заключается в определении единственного основания – специальной нормы об ответственности за действия с вредоносными компьютерными программами (ст. 320 УК КР).

4. Существенным пробелом уголовного законодательства Кыргызской Республики является отсутствие легального определения специальных технических средств в самом законе. Действующая конструкция ст. 266 УК КР, отсылающая к подзаконному акту (перечню, утверждаемому Кабинетом Министров) и Закону «Об оперативно-розыскной деятельности», нарушает принцип правовой определенности, имеющий совершенно особое значение для практики применения уголовного закона. Это создает риски расширительного толкования и проблематично при квалификации действий с вредоносными программами, которые, согласно межотраслевому толкованию, могут признаваться специальными техническими средствами. Возможное решение указанного пробела видится в имплементации в УК КР определения специальных технических средств по аналогии с российским подходом.

5. Обосновывается определение цифровой вредоносной программы – представленная в объективной форме совокупность цифровых данных и команд, предназначенных для несанкционированного функционирования любого

цифрового устройства, их систем или сетей, следствием чего является уничтожение, блокирование, модификация или копирование цифровой информации, нарушение работы устройств или сети.

6. Обосновывается несоответствие уголовного законодательства Российской Федерации и Кыргызской Республики положениям ст. 11 Конвенции ООН против киберпреступности в части криминализации оборота вредоносных программ и средств доступа к компьютерной информации.

7. В уголовном законодательстве Кыргызской Республики выявлен существенный пробел – отсутствие нормы, криминализующей оборот средств доступа к компьютерной информации. Это создает ситуацию, при которой деяния, являющиеся ключевым элементом подготовки к кибератакам (продажа баз данных с паролями, распространение фишинговых наборов), остаются вне сферы действия уголовного закона, если они не подпадают под признаки приготовления к конкретному преступлению.

8. Отсутствие в диспозициях уголовно-правовых норм указания на незаконность создает риск привлечения к ответственности специалистов по информационной безопасности, чья профессиональная деятельность неразрывно связана с использованием программ, обладающих техническими признаками вредоносности. В целях разграничения преступного и правомерного поведения требуется определять соответствующие диспозиции с обязательным указанием на незаконный характер деяний.

9. Обосновывается необходимость криминализации приобретения и (или) хранения вредоносных компьютерных программ (программных продуктов) в целях совершения иного преступления.

10. В уголовном законодательстве Российской Федерации и Республики Кыргызстан наличествует пробельность в части установления ответственности за создание и (или) обеспечение функционирования информационного ресурса (сайта в сети «Интернет» и (или) страницы сайта в сети «Интернет»), заведомо предназначенного для незаконных хранения, передачи (распространения, предоставления, доступа) цифровой информации, заведомо предназначенных для

несанкционированного уничтожения, блокирования, модификации, копирования цифровой информации или нейтрализации средств ее защиты.

Теоретическая и практическая значимость. Теоретическая значимость работы состоит в развитии положений науки уголовного права Российской Федерации, а также Кыргызской Республики на основе сравнительного анализа, в формулировании авторского подхода к пониманию признаков составов исследуемых преступлений.

Практическая значимость диссертации определяется возможностью использования полученных выводов и предложений в законотворческой деятельности Российской Федерации и Кыргызской Республики для совершенствования национального уголовного законодательства, а также в правоприменительной практике судов и следственных органов обеих стран. Материалы исследования могут быть использованы в учебном процессе юридических вузов при преподавании курсов уголовного права и специальных курсов по информационному праву и киберпреступности.

Степень достоверности результатов исследования. Достоверность полученных результатов обеспечивается методологией исследования, использованием диссертаций, а также трудов ведущих отечественных и зарубежных специалистов в области уголовного права, криминологии и информационной безопасности, что позволило обеспечить научную обоснованность выводов. В ходе сравнительно-правового анализа была изучена значительная база нормативных правовых актов, включая законодательство Российской Федерации и Кыргызской Республики, а также международные договоры и конвенции в сфере борьбы с киберпреступностью.

Эмпирическую базу исследования составляют:

– 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”», Методические рекомендации по осуществлению

прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации Генеральной прокуратуры Российской Федерации (в ред. от 13 сентября 2023 г.);

– 115 решений судов общей юрисдикции Российской Федерации, вынесенных по делам о создании, использовании и распространении вредоносных компьютерных программ. Из них 22 решения непосредственно включены в текст диссертации в качестве иллюстративного материала для обоснования теоретических положений;

– статистические данные, подготовленные ГИАЦ МВД России и Верховным судом Кыргызской Республики за период с 2021–2025 гг., а также полученные сведения о статистических данных по количеству совершаемых преступлений в сфере компьютерной информации за период 2021–2025 гг., в рамках официального запроса в Генеральную прокуратуру Кыргызской Республики;

– новостные публикации в газетах «РБК», «РИА Новости», «Sputnik», «Akipress», освещающие резонансные случаи распространения вредоносных программ (вирусов, троянов, программ-шифровальщиков, ботнетов). Данный материал использован для контекстуального анализа реальных угроз и оценки латентности исследуемых деяний;

– результаты анкетирования, в котором приняли участие 67 респондентов обоих государств.

Апробация результатов исследования. Основные положения и выводы настоящего исследования изложены автором в семи опубликованных работах общим объемом 3,94 п.л., в том числе 4 – в изданиях, рекомендованных Высшей аттестационной комиссией при Министерстве науки и высшего образования Российской Федерации, а также в выступлениях на региональных, всероссийских и международных научных и научно-практических мероприятиях: на Всероссийской научно-практической конференции «Казанские юридические чтения 2024» (18–19 апреля 2024 г., г. Казань), IV Международной научно-практической конференции «Цифровые технологии и право» (19 сентября 2025 г., г. Казань) и др.

Диссертация выполнена на кафедре уголовного права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА).

Структура диссертации определена целями и задачами исследования. Диссертация состоит из введения, трех глав, объединяющих восемь параграфов, заключения, списка использованных источников и литературы и приложений.

ГЛАВА 1. УГОЛОВНО-ПРАВОВОЕ ПРОТИВОДЕЙСТВИЕ СОЗДАНИЮ, ИСПОЛЬЗОВАНИЮ И РАСПРОСТРАНЕНИЮ ВРЕДОНОСНЫХ КОМПЬЮТЕРНЫХ ПРОГРАММ: ОБЩЕТЕОРЕТИЧЕСКИЙ АНАЛИЗ

§ 1. Состояние и основные направления противодействия киберпреступности в Российской Федерации и Кыргызской Республике

Общество находится в процессе активной цифровой трансформации, которая затрагивает все сферы человеческой жизни: экономику, политику, социальные отношения, культуру и право. Развитие информационных технологий и глобализация создали новые возможности для прогресса, но одновременно породили и новые угрозы, связанные с киберпреступностью[13].

Одним из основных векторов в государственной политике Российской Федерации и Кыргызской Республики является защита информационного пространства и киберпреступность.

В России Стратегия развития информационного общества на 2017– 2030 годы[14] подчеркивает важность защиты критической информационной инфраструктуры, создание отечественных технологий и обеспечение суверенитета в цифровом пространстве. Акцентируется внимание на замене иностранного программного обеспечения и оборудования отечественными аналогами, что позволит минимизировать риски несанкционированного доступа к данным, а также должно снизить зависимость от зарубежных технологий. Безусловно, большое значение уделяется противодействию компьютерным атакам, защите интересов граждан и государства, а также развитию технологий искусственного интеллекта (далее – ИИ) и больших данных.

---

[13] См.: Вострова А. Н. Развитие уголовного законодательства Кыргызской Республики об ответственности за киберпреступления // Расследование преступлений: проблемы и пути их решения. 2025. № 2. С. 143.

[14] Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // СЗ РФ. 2017. № 20. Ст. 2901.

Кыргызская Республика в своей Концепции цифровой трансформации на 2024–2028 годы также выделяет кибербезопасность как ключевое направление[15]. В документе подчеркивается необходимость защиты персональных данных, особенно в условиях активного использования биометрических идентификаторов. Особое значение уделяется развитию технологий блокчейна в целях обеспечения прозрачности процессов, например в избирательной системе, а также повышению осведомленности граждан и госслужащих о киберугрозах,

Важно отметить, что оба государства стремятся к созданию безопасной цифровой среды, но подходы несколько различаются. Россия делает упор на технологическую независимость и защиту критической инфраструктуры, в то время как Кыргызстан фокусируется на интеграции цифровых сервисов в государственное управление и повышении уровня цифровой грамотности населения. Однако, оба документа отражают общую тенденцию: цифровая трансформация невозможна без надежной системы кибербезопасности, которая должна развиваться параллельно с внедрением новых технологий.

Анализ динамики преступлений, предусмотренных ст. 273 УК РФ, показывает следующие изменения: в 2020 г. зарегистрировано 371 преступление (- 18,5%), в 2021 г. – 317 преступлений (-14,6%), в 2022 г. – 200 преступлений (- 36,9%), в 2023 г. – 196 преступлений (-2,0%), в 2024 г. – 309 преступлений (+57,7%) и в 2025 г. – 607 преступлений (+96,4%).

Уголовная политика в сфере киберпреступности в России и Кыргызстане формируется с учетом национальных особенностей, но оба государства признают необходимость международного сотрудничества и гармонизации законодательства для эффективного противодействия цифровым угрозам. Как подчеркивает Н.А. Лихачев, «проблематика преступлений, совершаемых в информационном пространстве, является приоритетным направлением уголовной политики из-за

---

[15] Указ Президента Кыргызской Республики от 5 апреля 2024 года УП № 90 «Об утверждении Концепции цифровой трансформации Кыргызской Республики на 2024–2028 годы» // Газета «Эркин-Тоо». 2024. 12 апр. № 90. [Электронный ресурс]. URL: https://cbd.minjust.gov.kg/5-10577/edition/6413/ru (дата обращения: 10.02.2025).

возросшей роли информации, встроившейся в систему общественных отношений»[16].

Уголовная политика является важнейшим элементом правового государства, направленным на защиту общественного порядка и интересов граждан через установление и реализацию уголовно-правовых норм[17]. Она включает в себя комплекс мероприятий, направленных на предупреждение, пресечение и наказание преступлений, а также на предотвращение негативных последствий преступной деятельности для общества в целом. В последние десятилетия особое внимание уделяется необходимости адаптации уголовной политики к новому вызову – киберпреступности, которая активно развивается на фоне глобализации информационных технологий.

Одним из составляющих элементов уголовной политики является уголовно-правовое направление, которое отражает состояние законодательного регулирования[18].

Безусловно, сам уголовный закон, определяющий основание и пределы ответственности за киберпреступления, является ключевым инструментом реализации уголовной политики в этой сфере. Как отмечает Е.А. Русскевич, уголовное законодательство является ведущим звеном механизма уголовно-правовой охраны[19].

В России первые нормы об уголовной ответственности за преступления в сфере компьютерной информации появились в 1996 г. в рамках гл. 28 «Преступления в сфере компьютерной информации», которая изначально содержала три статьи (ст. 272, 273, 274). В действующем уголовном законодательстве ответственность за преступления в сфере компьютерной

---

[16] Лихачев Н. А. Уголовно-правовое противодействие преступлениям в сфере обеспечения информационной безопасности: законодательный, правоприменительный и доктринальный аспекты: дис. …канд. юрид. наук. Краснодар, 2024. С. 6.

[17] См.: Голик Ю. В., Коробеев А. И., Усс А. В. Уголовно-правовая политика. Тенденции и перспективы. Красноярск, 1991. С. 7.

[18] См.: Лопашенко Н. А. Уголовная политика. М., 2009. С. 29.

[19] См.: Русскевич Е. А. Уголовное право и «цифровая преступность»: проблемы и решения: монография. 2-е изд., перераб. и доп. М., 2023. С. 11.

информации по-прежнему предусмотрена в гл. 28 УК РФ, которая содержит уже девять статей.

1. Неправомерный доступ к компьютерной информации (ст. 272).

2. Незаконные использование и (или) передача, сбор и (или) хранение компьютерной информации, содержащей персональные данные, а также создание и (или) обеспечение функционирования информационных ресурсов, предназначенных для ее незаконного хранения и (или) распространения (ст. 272^1).

3. Создание, использование и распространение вредоносных компьютерных программ (ст. 273).

4. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно телекоммуникационных сетей (ст. 274).

5. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274^1).

6. Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования (ст. 274^2).

7. Незаконное использование абонентского терминала пропуска трафика или виртуальной телефонной станции (ст. 274^3).

8. Организация деятельности по передаче абонентских номеров с нарушением требований законодательства Российской Федерации (ст. 274^4).

9. Организация деятельности по передаче информации, необходимой для регистрации и (или) авторизации пользователя сети «Интернет» для получения доступа к функциональным возможностям информационного ресурса (ст. 274^5).

В 2017 г. законодателем в гл. 28 УК РФ была введена ст. 274^1 «Неправомерное воздействие на критическую информационную инфраструктуру

Российской Федерации»[20]. Согласно пояснительной записке к проекту закона[21] включение соответствующей нормы отражает стремление законодателя усилить защиту критически важных информационных систем, что обусловлено возрастающей ролью цифровых технологий и увеличением киберугроз. Законодатель указывает на необходимость выделения новых составов преступлений, связанных с критической информационной инфраструктурой, в отдельную статью, повышенной общественной опасностью соответствующих деяний. В связи с тем, что речь идет о комплексной защите информационных систем, функционирование которых критически важно для устойчивого развития экономики, обороны, безопасности, здравоохранения, транспорта, связи и других жизненно значимых отраслей.

Действительно, имеющиеся уголовно-правовые нормы об ответственности за преступления в сфере компьютерной информации не в полной мере учитывали специфику и значимость критической информационной инфраструктуры. Введение ст. 274^1 УК РФ позволяет дифференцировать ответственность за неправомерное воздействие на такие системы, что соответствует тенденции цифровой специализации уголовно-правовых норм в условиях технологического развития.

В последующем гл. 28 УК РФ была дополнена ст. 274^2 УК РФ, данная норма служит инструментом охраны централизованного управления техническими средствами, предназначенными для обеспечения устойчивости, безопасности и целостности информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования. Введенная новелла является неким подтверждением о

---

[20] Федеральный закон от 26 июля 2017 г. № 194-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона “О безопасности критической информационной инфраструктуры Российской Федерации”» // СЗ РФ. 2017. № 31 (ч. 1). Ст. 4743.

[21] Пояснительная записка к Проекту постановления Правительства РФ «Об утверждении правил проверки соответствия пользователей государственной информационной системы, определенной в соответствии с частью 2 статьи 13.1 Федерального закона “О персональных данных”, требованиям, указанным в части 7 статьи 13.1 Федерального закона “О персональных данных” о внесении изменений в некоторые акты Правительства Российской Федерации» (подготовлен Минцифры России, ID проекта 01/01/02-25/00154667). URL: https://www.garant.ru/products/ipo/prime/doc/56914908/ (дата обращения: 10.02.2025).

проводимой политики в последние годы криминализации нарушений, связанной с функционированием критически значимой информационной инфраструктуры

Я.Н. Ермолович пишет о том, что норма носит формальный, бланкетный характер и включает административную преюдицию, что делает ее зависимой от содержания и применения норм Кодекса РФ об административных правонарушениях (далее – КоАП РФ), в частности ч. 2 ст. 13.42 и ст. 13.42.1, а также подчеркивает необходимость четкого указания в обвинительном акте на конкретные нормативные акты, положения которых были нарушены, поскольку без такой конкретизации дело не может быть рассмотрено судом по существу и должно быть возвращено прокурору в порядке ст. 237 Уголовно-процессуальноо кодекса РФ (далее – УПК РФ)[22].

С точки зрения уголовно-правовой политики, введение ст. 274^2 УК РФ можно оценить, как пример расширения охранительных механизмов государства в сфере цифрового регулирования.

Вместе с тем важно указать на то, что ст. 274^2 УК РФ порождает риски произвольного толкования, особенно в условиях отсутствия четкого определения «нарушения правил централизованного управления». П.С. Яни подчеркивает, что подобные бланкетные нормы с формальным составом, как правило, страдают неопределенностью пределов применения, что может подрывать принцип правовой определенности, закрепленный в Конституции РФ, и указывает на то, что отсутствие в ст. 274^2 УК РФ «размерных» признаков (например, тяжести наступивших последствий или объема неисполненных обязанностей) делает ее чрезмерно широкой и потенциально уязвимой для произвольного толкования[23]. Пожалуй, что опасения П.С. Яни являются далеко не беспочвенными, в связи с тем, что действующая редакция 274^2 УК РФ может привести к привлечению к уголовной ответственности за деяния, которые не представляют значительной

[22] См.: Ермолович Я. Н. Научно-практический комментарий к Федеральному закону «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации» от 14 июля 2022 года № 260-ФЗ // Право в Вооруженных Силах. 2022. № 11. С. 95.

[23] См.: Яни П. С. Проблемы квалификации преступлений в сфере гособоронзаказа // Законность. 2023. № 9. С. 46.

общественной опасности, тем самым появляются предпосылки для нарушения принципа справедливости наказания.

При этом особое внимание вызывает вопрос о субъекте нарушения правил централизованного управления. Согласно закону им является должностное лицо или индивидуальный предприниматель, выполняющие организационно-распорядительные или административно-хозяйственные функции в организации. Такое определение субъекта может вызывать сложности на практике, особенно в части отграничения от субъектов, предусмотренных, например, ст. 285 УК РФ. Это также может создавать проблемы с разграничением административной и уголовной ответственности, особенно в свете обязательной административной преюдиции: лицо может быть привлечено к уголовной ответственности только при наличии ранее совершенного аналогичного административного правонарушения.

Таким образом, можно сказать, что ст. 274^2 УК РФ отражает своего рода тенденцию современной уголовной политики России в виде усиления уголовно-правового контроля за цифровой сферой, особенно в ее инфраструктурном аспектах. При этом вполне очевидно, что само решение российского законодателя страдает рядом недостатков, характерных в целом для многих бланкетных норм – отсутствием четких критериев применения, неопределенностью диспозиции и потенциальной конкуренцией с нормами административного законодательства.

В 2024 г. законодатель дополнил гл. 28 УК РФ новой ст. 272^1 «Незаконные использование и (или) передача, сбор и (или) хранение компьютерной информации, содержащей персональные данные, а также создание и (или) обеспечение функционирования информационных ресурсов, предназначенных для ее незаконного хранения и (или) распространения»[24].

[24] Федеральный закон от 30 ноября 2024 г. № 421-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» // СЗ РФ. 2024. № 49 (ч. 4). Ст. 7412.

Анализ пояснительной записки[25] позволяет сделать вывод о том, что данная законодательная инициатива является реакцией государства на стремительно нарастающие угрозы, связанные с незаконным оборотом персональных данных в цифровой среде. Статья вводится в условиях устойчивого роста преступности в России, связанной с использованием информационно-телекоммуникационных технологий, и фиксируемого ежегодного увеличения числа утечек, объемов нелегального оборота баз данных и их последующего распространения в теневых сегментах сети «Интернет». По данным, приведенным в пояснительной записке, масштабы таких преступлений приобрели системный характер и наносят серьезный ущерб частной жизни граждан, правопорядку и экономической безопасности государства.

Несоответствие нынешних уголовно-правовых норм масштабу и характеру совершаемых преступлений является одним из основных мотивов введения нового состава преступления в УК РФ. Как отмечено, что действующие составы не охватывают всех общественно опасных форм поведения, связанных с незаконным использованием персональных данных, особенно когда речь идет о действиях с компьютерной информацией, полученной в обход систем защиты либо посредством неправомерного доступа. В этом контексте новая ст. 272[1] УК РФ призвана восполнить существующие пробелы и обеспечить уголовно-правовую защиту персональных данных в условиях цифровой трансформации общества.

В данной статье законодатель выделяет основной состав – это незаконное использование, сбор, хранение и передача компьютерной информации, содержащей персональные данные, а также квалифицированный составы, где за них предусмотрены более строгие санкции, если преступление совершено группой лиц, с использованием служебного положения, из корыстной заинтересованности, а также при трансграничной передаче данных. На наш взгляд, настоящая структура

[25] Пояснительная записка к проекту федерального закона № 502113-8 «О внесении изменений в Уголовный кодекс Российской Федерации» (ред., внесенная в ГД ФС РФ, текст по состоянию на 04.12.2023) // Государственная Дума Федерального Собрания Российской Федерации. Система обеспечения законодательной деятельности (СОЗД). URL: https://sozd.duma.gov.ru/bill/502113-8 (дата обращения: 10.05.2025).

статьи, с одной стороны, позволяет более гибко реализовывать уголовную ответственность, а с другой обеспечить соответствие принципу справедливости.

Важно, что в комментируемой новелле предметом посягательства выступает именно компьютерная информация с персональными данными, *полученная незаконным путем*. Это позволяет разграничить сферу действия ст. 272^1 УК РФ от административных правонарушений (например, ст. 13.11 КоАП РФ) и иных преступлений, связанных с вмешательством в сферу частной жизни. Одновременно законопроект предусматривает исключение для правомерного использования персональных данных в личных и семейных целях – и это, думается, важная гарантия против чрезмерной криминализации.

Пожалуй, отдельного внимания заслуживает усиление ответственности за действия, связанные с администрированием Интернет-ресурсов, предназначенных для хранения и распространения похищенных персональных данных (ч. 6 ст. 272^1 УК РФ). По сути, речь идет о криминализации организации инфраструктуры, обеспечивающей незаконный оборот персональной информации, что вполне соответствует современным тенденциям развития уголовного законодательства в сфере кибербезопасности. Такая мера отражает необходимость пресекать не только отдельные акты, но и бороться с устойчивыми каналами незаконного оборота данных.

Как следует из пояснительно записки, законопроект носит системный характер: он сопровождался параллельными инициативами по ужесточению административной ответственности операторов персональных данных. Вследствие чего, уголовно-правовая мера встраивается в более широкий комплексный механизм регулирования, направленный на предупреждение правонарушений, защиту прав граждан и соблюдение информационной безопасности.

С точки зрения уголовно-правовой политики ст. 272^1 УК РФ, которая отражает тенденцию к усилению охраны цифровых прав личности и приоритету информационной безопасности как элемента национальной безопасности.

Комплекс правок, который был введен гл. 28 УК РФ в 2025 году демонстрирует иную реакцию на вызовы, порождаемые процессами

цифровизации. Так, Федеральный закон от 31 июля 2025 г. № 282-ФЗ[26], вступивший в силу с 1 сентября 2025 г., существенно обновил уголовно-правовой инструмент в борьбе с киберпреступностью, а именно посредством криминализации новых видов общественно опасных деяний. Настоящая реформа выражается в введение трех новых составов преступлений, которые направлены на пресечение каналов анонимизации и технического обеспечения противоправной деятельности в телекоммуникационных сетях:

– уголовная ответственность за незаконное использование абонентского терминала пропуска трафика или виртуальной автоматической телефонной станции (далее – АТС), если эти действия сопряжены с целью совершения иного преступления или повлекли тяжкие последствия (ст. 274^3 УК РФ);

– уголовная ответственность за организацию деятельности по передаче абонентских номеров с нарушением законодательства, совершенную из корыстной заинтересованности или в преступных целях (ст. 274^4 УК РФ);

– уголовная ответственность за деятельность направленную против организации деятельности по передаче данных для регистрации и авторизации в сети «Интернет», что блокирует один из ключевых элементов теневого оборота цифровых идентификаторов (ст. 274^5 УК РФ).

В российской доктрине уголовного права справедливо отмечено, что общественная опасность деяния, предусмотренного ст. 274^3 УК РФ, проявляется в его инструментальной роли для совершения преступлений, прежде всего массовых дистанционных мошенничеств, а также в причинении вреда телекоммуникационной инфраструктуре и подрыве доверия к цифровым коммуникациям[27].

---

[26] Федеральный закон от 31 июля 2025 г. № 282-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статьи 31 и 151 Уголовно-процессуального кодекса Российской Федерации» // Официальный интернет-портал правовой информации. URL: http://publication.pravo.gov.ru/document/0001202507310013 (дата обращения: 20.12.2025).

[27] См.: Кравчук С. В. К вопросу о социальной обусловленности криминализации незаконного использования абонентского терминала пропуска трафика или виртуальной телефонной станции // Проблемы права. 2025. № 4 (100). С. 130.

Введение отечественным законодателем уголовной ответственности за деяние, предусмотренное ст. 274^4 УК РФ, также обусловлено ее инфраструктурным характером. Данное деяние само по себе редко причиняет прямой ущерб, но систематически создает технические и организационные условия для совершения широкого спектра преступлений: от дистанционных мошенничеств и деятельности «серых» call-центров до легализации преступных доходов и содействия террористической деятельности[28].

Параллельно усложнена и дифференциация ответственности за совершение преступлений с использованием специализированных технических средств. Дополнение пунктом «ф» ч. 1 ст. 63 УК РФ, в соответствии с которым признается отягчающим обстоятельством применение программно-аппаратных средств для доступа к ограниченным информационным ресурсам и сетям, ориентировано на повышение уровня наказания для лиц, использующих так называемые анонимайзеры для обхода систем защиты.

Нетрудно заметить, что данные уголовно-правовые нормы в целом призваны обеспечить соблюдение регуляторных режимов в области связи. И в этом отношении надо сказать о том, что действующее наименование гл. 28 УК РФ уже не в полной мере отражает ее актуальное содержание.

В целом же реформа 2025 г. знаменует собой качественно новый этап развития российского уголовного законодательства в области обеспечения кибербезопасности.

Однако же, думается, что новеллы гл. 28 УК РФ имеют «две стороны медали». В этой связи уместно сослаться на мнение Н.Ш. Козаева, который справедливо пишет: «Одной из ключевых проблем законодательной техники в уголовном праве сегодня является запаздывание правовой регламентации по сравнению с динамично изменяющимися социально-экономическими отношениями. Формирование адекватной правовой базы противодействия

---

[28] См.: Захарян С. Ю. Основания криминализации и социальная обусловленность организации деятельности по передаче абонентских номеров с нарушением требований законодательства Российской Федерации // Проблемы права. 2025. № 4 (100). С. 110.

преступности в условиях научно-технического прогресса служит не только гарантией национальной безопасности, но и укрепляет авторитет России как стратегического партнера в сфере внешней политики и международных экономических отношений»[29].

В Кыргызской Республике уголовная ответственность за преступления в сфере компьютерной информации впервые появилась с принятием Уголовного кодекса Кыргызской Республики 1 октября 1997 г. № 68[30]. Глава 28 «Преступления в сфере компьютерной информации» включала в себя три статьи.

1. Неправомерный доступ к компьютерной информации (ст. 289 УК КР).

2. Создание, использование и распространение вредоносных программ для ЭВМ (ст. 290 УК КР).

3. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 291 УК КР).

В 2017 г. был принят новый УК КР[31], который, однако, недолго действовал, во многом из-за недостаточного научного сопровождения законотворческого процесса[32].

В 2021 г. уголовное законодательство о компьютерных преступлениях Кыргызской Республики претерпело значительные изменения. В частности, появились новые составы: киберсаботаж и массовое распространение электронных сообщений. Прогрессивные изменения произошли в части терминологии и выразились в отказе от устаревших терминов (ЭВМ и др.)[33]. В действующем уголовном законодательстве Кыргызской Республики ответственность за

---

[29] Козаев Н. Ш. Современные технологии и проблемы уголовного права (анализ зарубежного и российского законодательства): монография / под ред. А. В. Наумова. М., 2015. С. 7.

[30] Уголовный кодекс Кыргызской Республики от 1 октября 1997 г. № 68 (утратил силу с 1 января 2019 г. в соответствии с Законом Кыргызской Республики от 24 января 2017 г. № 10) [Электронный ресурс]. URL: https://cbd.minjust.gov.kg/3-10/edition/919984/ru (дата обращения: 15.05.2025).

[31] Уголовный кодекс Кыргызской Республики от 2 февраля 2017 г. № 19 (утратил силу в соответствии с Законом Кыргызской Республики от 28 октября 2021 г. № 126) [Электронный ресурс]. URL: https://cbd.minjust.gov.kg/111527/edition/1186183/ru (дата обращения: 09.04.2025)

[32] См.: Атабеков К. К. Новое уголовное законодательство Кыргызской Республики: предпосылки принятия и некоторые его коллизии // Экономика. Право. Общество. 2024. Т. 9. № 1. С. 84.

[33] См.: Вострова А. Н. Указ. соч. С. 144.

компьютерные преступления предусмотрена в гл. 40 УК «Преступления против кибербезопасности», которая содержит четыре статьи.

1. Несанкционированный доступ к компьютерной информации и электронным документам, в информационную систему или сеть электросвязи (ст. 319 УК КР).

2. Создание вредоносных программных продуктов (ст. 320 УК КР).

3. Киберсаботаж (ст. 321 УК КР).

4. Массовое распространение электронных сообщений (ст. 322 УК КР).

Введение нового УК КР в 2021 г. было вызвано рядом системных проблем, выявленных при применении предыдущего законодательства, а также необходимостью привести его в соответствие с изменившимся конституционным и правовым полем страны[34].

Инициатором реформы выступил Генеральный прокурор Кыргызской Республики, получивший право законодательной инициативы в соответствии со ст. 85 Конституции Кыргызской Республики[35]. Основными причинами обновления Кодекса стали: наличие многочисленных коллизий и противоречий в действующем законодательстве, что подтверждается внесением 285 изменений в Кодекс за два года, не устранивших проблему волокиты и несправедливых решений; проблемы в практике назначения наказаний, когда суды вынуждены были назначать лишение свободы ранее несудимым, а санкции, сочетающие штраф и лишение свободы, на практике не исполнялись, нарушая принцип справедливости; недостатки в регулировании отдельных процессуальных институтов, например отсутствие четких норм о возбуждении уголовных дел, что вело к затягиванию следствия[36].

---

[34] Сажать без штрафов и отменить Кодекс о проступках – проект нового УК КР. URL: https://ru.sputnik.kg/20210510/kyrgyzstan-ugolovnyy-kodeks-izmeneniya-1052449627.html (дата обращения: 25.12.2025).

[35] Закон Кыргызской Республики от 5 мая 2021 года № 59 «О Конституции Кыргызской Республики» // Газета «Эркин-Тоо». 2021. 7 мая. № 64. URL: https://cbd.minjust.gov.kg/1-2/edition/1202952/ru (дата обращения: 25.12.2025).

[36] Новое уголовное законодательство Кыргызстана: откат назад или курс на результативность? URL: https://cabar.asia/ru/novoe-ugolovnoe-zakonodatelstvo-kyrgyzstana-otkat-nazad-ili-kurs-na-rezultativnost (дата обращения: 25.12.2025).

На сегодняшний день в Кыргызской Республике осуществляется активное правотворчество в отношении урегулирования цифровой среды. Так, 17 июля 2024 г. был принят Закон КР «О кибербезопасности Кыргызской Республики»[37], который устанавливает правовые основы единой системы кибербезопасности, направленной на защиту личности, общества и государства путем обеспечения цифровой устойчивости информационной инфраструктуры, а также введение Цифрового кодекса Кыргызской Республики (далее – ЦК КР)[38].

Анализ действующей нормативной базы показал, что в Кыргызской Республике отсутствует системный подход к регулированию цифровых отношений. Более 100 нормативных актов, касающихся связи, телекоммуникаций, защиты данных, кибербезопасности и других аспектов цифровизации, разрознены и зачастую противоречат друг другу. Это создает препятствия для развития цифровой экономики, внедрения инновационных технологий, таких как ИИ, блокчейн, большие данные, а также для эффективного государственного управления[39].

Безусловно, нельзя оставить без внимания, что в настоящее время наблюдается стремительное нарастание дискурса вокруг таких понятий, как «цифровой», «цифровая информация», «цифровая среда», что является закономерным отражением глубинной трансформации всех сфер жизни под воздействием информационных технологий. В данном контексте ключевые вопросы кибербезопасности требуют особой концептуальной четкости.

В рамках настоящего исследования, чтобы понять эволюцию юридической мысли о «вредоносных программах» необходимо углубиться в историю появления

---

[37] Закон Кыргызской Республики от 17 июля 2024 г. № 121 «О кибербезопасности Кыргызской Республики» // Газета «Эркин-Тоо». 2024. 19 июля. № 123. URL: https://cbd.minjust.gov.kg/4-5371/edition/13381/ru (дата обращения: 15.10.2025).

[38] Кодекс Кыргызской Республики от 31 июля 2025 г. № 178 «Цифровой кодекс Кыргызской Республики». URL: https://cbd.minjust.gov.kg/3-48/edition/35412/ru?lang=ru (дата обращения: 25.02.2025).

[39] См.: Справка-обоснование к проекту Цифрового кодекса Кыргызской Республики, № 6-6296/24, 18-06-2024. URL: https://kenesh.kg/bills/653899 (дата обращения: 01.03.2025).

и развития этого термина в уголовном законодательстве Российской Федерации и Кыргызской Республики.

Эволюция термина «вредоносные программы» в уголовном законодательстве России и Кыргызстана демонстрирует как общие закономерности, обусловленные развитием информационных технологий, так и существенные различия в подходах к юридической технике.

Формирование этого термина в российском законодательстве прошло несколько этапов. Как подробно описывает К.Н. Евдокимов, превичные попытки криминализации, которые были предприняты еще в проекте Закона РСФСР «Об ответственности за правонарушения при работе с информацией» от 6 декабря 1991 г., фигурировал термин «компьютерный вирус» вместо «вредоносных программ», что существенно сужало сферу уголовно-правовой охраны[40]. Термин «вредоносная программа», впервые получил законодательное закрепление, в связи с принятием УК РФ в 1996 г., когда ст. 273 «Создание, использование и распространение вредоносных программ для ЭВМ» стала первой нормой, которая была направлена на борьбу с киберпреступностью.

Дальнейшее развитие технологий и появление новых угроз привели к расширению сферы применения данного термина. Так, в 2017 г. с введением ст. 274[1] УК РФ, предусматривающей ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации, законодатель распространил указание на вредоносные программы и на этот особо значимый объект. Впоследствии, в 2019 г., упоминание про программное обеспечение нашло свое отражение и в примечании 1 к ст. 138[1] УК РФ, где было уточнено, что понимается под специальными техническими средствами, предназначенными для негласного получения информации, что также коррелирует с их возможным вредоносным потенциалом.

---

[40] См.: Евдокимов К. Н. Создание, использование и распространение вредоносных компьютерных программ: уголовно-правовые и криминологические аспекты : монография. Иркутск, 2013. С. 88.

Что касается Кыргызской Республики, то здесь эволюция термина оказалась более динамичной и прошла через три последовательных этапа, отражающих смену уголовных кодексов и развитие законодательной техники.

Впервые упоминание о «вредоносных программах» было закреплено в 1997 г. в ст. 290 УК КР 1997 г., которая называлась «Создание, использование и распространение вредоносных программ для ЭВМ». Как видно, данный этап в целом соответствовал и российскому подходу на начало 1990-х гг.

Следующий этап связан с принятием УК КР 2017 г., где вместо термина «вредоносные программы для ЭВМ» законодатель использовал в ст. 305 УК КР 2017 г. термин «вредоносные компьютерные программы».

Наконец, после принятия УК КР 2021 г. произошла очередная терминологическая трансформация: вместо «вредоносных компьютерных программ» стали использовать в ст. 320 УК КР 2021 г. термин «создание вредоносных программных продуктов».

Аналогом российской ст. 138^1 УК РФ в законодательстве Кыргызстана выступает ст. 266 УК КР «Незаконные производство и оборот специальных технических средств», которая устанавливает ответственность за незаконные производство, сбыт или приобретение в целях сбыта специальных технических средств, предназначенных для негласного получения информации. Принципиальное различие заключается в том, что в уголовном законодательстве Кыргызстана отсутствует определение того, что понимается под специальными техническими средствами, однако в примечании к ст. 266 УК КР указано, что *перечень таких средств утверждается Кабинетом Министров Кыргызской Республики*. Именно здесь кроется существенное различие в законодательной технике двух стран и, думается, серьезный пробел в законодательстве Кыргызской Республике.

Данный перечень закреплен в постановлении Правительства Кыргызской Республики от 7 августа 2014 г. № 451 «Об утверждении Перечня видов специальных технических средств, предназначенных для негласного получения информации в процессе осуществления оперативно-розыскной и

контрразведывательной деятельности, а также применяемых при производстве специальных следственных действий»[41]. При этом само постановление не содержит определения специальных технических средств. Оно раскрывается в п. 5 ст. 2 Закона Кыргызской Республики «Об оперативно-розыскной деятельности»[42], который определяет специальные технические средства как устройства, аппаратуру, приспособления, оборудование, имеющие специальные функции, *программное обеспечение* и конструктивные особенности для добывания и документирования информации в ходе проведения оперативно-розыскных мероприятий, в том числе в сетях (на каналах) связи. Согласно данному определению программное обеспечение признается специальным техническим средством, что создает интересный правовой прецедент, когда вредоносные программы могут квалифицироваться и по статье о специальных технических средствах в зависимости от их функционального предназначения.

Соответственно, складывается следующая ситуация, где содержание раскрывается через призму отсылок: от уголовного кодекса к подзаконному акту, а от него к специальному закону, который не является непосредственным источником уголовного права. Безусловно, это затрудняет процесс правоприменения, который можно воспринимать за дефект законодательства. Данный факт нарушает принцип правовой определенности, требующий, чтобы уголовный закон должен быть ясным, четким и не допускал расширительного толкования. Российский же подход, где дефиниция закреплена прямо в примечании к норме, выглядит более удачным с точки зрения законодательной техники и даёт лучшую правовую защищенность.

---

[41] Постановление Правительства Кыргызской Республики от 7 августа 2014 г. № 451 «Об утверждении Перечня видов специальных технических средств, предназначенных для негласного получения информации в процессе осуществления оперативно-розыскной и контрразведывательной деятельности, а также применяемых при производстве специальных следственных действий» // Газета «Эркин-Тоо». 2014. 12 авг. № 451. URL: https://cbd.minjust.gov.kg/7-17460/edition/1249991/ru (дата обращения: 20.02.2026).

[42] Закон Кыргызской Республики от 26 июня 2025 г. № 127 «Об оперативно-розыскной деятельности» // Газета «Эркин-Тоо». 2025. 1 июля. № 141. URL: https://cbd.minjust.gov.kg/4-5574/edition/34556/ru (дата обращения: 20.02.2026).

Думается, что в этой части подход российского законодателя является более обоснованным и может быть воспринят в практике законотворческой деятельности Кыргызстана. При этом соответствующее примечание 1 к ст. 266 УК КР могло бы быть представлено следующим образом: «Под специальными техническими средствами, предназначенными для негласного получения информации, в настоящем Кодексе понимаются приборы, системы, комплексы, устройства, специальные инструменты для проникновения в помещения и (или) на другие объекты и программные продукты для электронных вычислительных машин и других электронных устройств для доступа к информации и (или) получения информации с технических средств ее хранения, обработки и (или) передачи, которым намеренно приданы свойства для обеспечения функции скрытого получения информации либо доступа к ней без ведома ее обладателя».

Такое законодательное решение, аналогичное российскому подходу, позволило бы устранить выявленный пробел, обеспечить соответствие уголовного закона принципу правовой определенности и создать прочную основу для единообразной правоприменительной практики, особенно в части квалификации вредоносного программного обеспечения как специального технического средства. В отличие от действующей системы отсылок, российский подход с закреплением дефиниции непосредственно в примечании к уголовно-правовой норме представляется более совершенным с точки зрения законодательной техники и обеспечивающим большую правовую защищенность граждан и организаций.

В завершение важно указать на то, что значимой вехой российской уголовной политики в сфере противодействия киберпреступности стало принятие Пленумом Верховного Суда РФ постановления от 15 декабря 2022 г. № 37. В данном документе Верховный Суд РФ сформулировал несколько прогрессивных позиций, конкретизирующих положения гл. 28 УК РФ. В частности, впервые было определено специальное правило, согласно которому не содержит признаков преступления создание и (или) использование вредоносных компьютерных программ лицом на принадлежащих ему компьютерных устройствах либо с согласия собственника компьютерного устройства, если такие действия не

преследуют цели неправомерного доступа к охраняемой законом компьютерной информации и не повлекли несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств ее защиты, например, в образовательных целях либо в ходе тестирования компьютерных систем для проверки уязвимости средств информации, к которым у данного лица имеется правомерный доступ[43].

В Кыргызстане соответствующих разъяснений со стороны высшей судебной инстанции не выработано, что во многом объясняется отсутствием самой практики по ст. 320 УК КР. Вместе с тем в этом отношении нельзя не обратить внимания на полезность российского опыта в части формирования единообразной практики в будущем.

§ 2. Международный опыт противодействия киберпреступности

Председатель Совета министров внутренних дел (далее – СМВД) государств – участников Содружества Независимых Государств, министр внутренних дел Кыргызской Республики генерал-лейтенант милиции У.О. Ниязбеков на саммите СМВД в сентябре 2022 г. отметил, что криминальная ситуация на пространстве Содружества претерпевает активную трансформацию. Традиционные формы преступности уступают место новым, более сложным видам противоправной деятельности, совершаемым с использованием IT-технологий. Эти преступления отличаются высокой вариативностью, латентностью и трансграничным характером, что усложняет их выявление и расследование[44].

---

[43] 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». URL: https://www.consultant.ru/document/cons_doc_LAW_434573/ (дата обращения: 15.02.2025).

[44] См.: Сборник актуальных документов Совета Министров внутренних дел. М., 2022. № 3. С. 90 URL: https://mvd.gov.kg/media/gender_politic/%D0%A1%D0%B1%D0%BE%D1%80%D0%BD%0%B8%D0%BA_%D1%80%D0%B5%D1%88%D0%B5%D0%BD%D0%B8%D0%B9_%D0%A1%D0%9C%D0%92%D0%94_2019-2022_3.pdf (дата обращения: 16.02.2026).

Стоит согласиться с мнением А.Ж. Саркисяна, который пишет, что «в условиях стремительного развития информационно-коммуникационные технологии (далее – ИКТ) и увеличения числа киберугроз международное сотрудничество и координация усилий становятся ключевыми элементами в борьбе с киберпреступностью»[45]. В связи с этим особую актуальность приобретает укрепление международного сотрудничества, направленного на противодействие киберпреступности. Важную роль в этом процессе играют такие организации, как Организация Объединенных Наций (далее – ООН), Содружество Независимых Государств (далее – СНГ), Шанхайская организация сотрудничества (далее – ШОС), Лига арабских государств (далее – ЛАГ), Африканский союз (далее – АС), Объединение БРИКС (Бразилия, Россия, Индия, Китай и Южно-Африканская Республика (ЮАР)) (далее – БРИКС), которые разрабатывают стратегии, стандарты и конкретные механизмы взаимодействия в борьбе с цифровыми угрозами.

В 1990 г. в Гаване на IX Конгрессе ООН по предупреждению преступности была обозначена проблема компьютерной преступности[46].

Знаковым событием стало принятие Будапештской конвенции о киберпреступности в 2001 г. (далее – Будапештская конвенция 2001 г.) Советом Европы (далее – СЕ)[47], которая установила первые ориентиры на международном уровне в данной области.

Безусловно, Будапештская конвенция 2001 г. стимулировала развитие национального законодательства относительно противодействия киберпреступности[48]. Изложенные принципы в Будапештской конвенции 2001 г.

---

[45] Саркисян А. Ж. Транснациональный характер преступности в киберпространстве // Расследование преступлений: проблемы и пути их решения. 2024. № 3. С. 74.

[46] См.: Материалы IX Конгресса ООН по предупреждению преступности и обращению с правонарушителями. URL: http: www.un.org (дата обращения: 09.01.2025).

[47] Конвенция о преступности в сфере компьютерной информации от 23 ноября 2001 г. ETS № 185 // ЭПС «Система ГАРАНТ». [Электронный ресурс]. – URL: http://base.garant.ru/4089723 (дата обращения: 09.01.2025).

[48] См.: Шестак В.А., Чеботарь А.С. Будапештская конвенция как основополагающий механизм противодействия киберпреступности: новации и перспективы международно-правового регулирования // Образование и право. 2023. № 8. С. 305–310.

стали основой для большинства типовых законодательных актов по противодействию киберпреступности международного и национального уровня.

На сегодняшний день не является открытием тот факт, что компьютерные системы являются не только объектом противоправного воздействия, но и могут быть орудием совершения преступления. В Будапештской конвенции 2001 г. были определены четыре группы преступлений, связанные с ИКТ.

Первую группу составляют такие противоправные деяния, как незаконный доступ, незаконный перехват, вмешательство в данные, вмешательство в систему, которые направлены напрямую против конфиденциальности, доступности и целостности компьютерных систем и данных. Настоящие составы являются классическими преступлениями, где компьютерная система является основным объектом посягательства.

Вторую группу охватывают преступления, связанные с использованием компьютерных систем как инструмента для совершения традиционных правонарушений. К таковым можно отнести, например, компьютерные мошенничества или преступления, связанные детской порнографией. Основная суть заключается в облегчении или расширении возможностей совершения противоправных деяний.

К третьей группе относятся преступления, которые связаны с содержанием данных, например распространение вредоносного контента, включая пропаганду терроризма или разжигание ненависти. Основной акцент фокусируется на информационном наполнении, которое может причинить вред обществу или отдельным лицам.

Четвертую группу составляют такие правонарушения, которые связаны с нарушением в цифровой среде авторских или смежных прав, что отражает растущую значимость защиты интеллектуальной собственности в нынешних условиях.

В контексте настоящего исследования особый интерес представляют первая и вторая группы, поскольку именно они охватывают деяния, совершаемые с использованием вредоносных программ – как непосредственное воздействие на

информационные системы, так и использование вредоносного программного обеспечения как инструмента для мошенничества и иных преступлений.

Будапештская конвенция 2001 г. также ввела важные процессуальные нормы, направленные на облегчение международного сотрудничества в расследовании киберпреступлений. Речь идет о механизмах быстрого сохранения данных, взаимной правовой помощи, экстрадиции и совместных расследованиях. Эти положения стали основой для многих национальных законодательств, которые начали включать аналогичные инструменты в свои правовые системы.

Несмотря на то что Российская Федерация приняла решение о подписании Будапештской конвенции 2001 г. о киберпреступности[49], процесс ее ратификации так и не был завершен[50]. Основные претензии касались механизмов международного сотрудничества, в частности, обязательств по предоставлению данных по запросам иностранных правоохранительных органов, что, по мнению России, создавало угрозу вмешательства во внутренние дела государства[51].

В 2022 г. Совет Европы принял Второй дополнительный Протокол к Будапештской конвенции 2001 г.[52], направленный на расширение международного сотрудничества, особенно между правоохранительными органами и частным сектором. Он предполагает более гибкие механизмы прямого обмена информацией, в том числе между государствами и поставщиками интернет-услуг, однако по-прежнему вызывает опасения в вопросах защиты персональных данных и юрисдикции.

---

[49] См.: Распоряжение Президента РФ от 15 ноября 2005 г. № 557-рп «О подписании Конвенции о киберпреступности» // СЗ РФ. 2005. № 47. Ст. 4929.

[50] См.: Распоряжение Президента РФ от 22 марта 2008 г. № 144-рп «О признании утратившим силу распоряжения Президента Российской Федерации от 15 ноября 2005 г. № 557-рп “О подписании Конвенции о киберпреступности”» // СЗ РФ. 2008. № 13. Ст. 1295.

[51] См.: Доклад Генерального секретаря ООН от 30 июля 2019 г. в соответствии с Резолюцией Генеральной Ассамблеи ООН A/RES/73/187 от 17 декабря 2018 г., озаглавленной «Противодействие использованию информационно-коммуникационных технологий в преступных целях» // Официальный сайт ООН. URL: https://docs.un.org/ru/A/74/130 (дата обращения: 15.03.2025).

[52] URL: https://www.coe.int/en/web/deputy-secretary-general/-/treaty-signature-ceremony-of-the-second-additional-protocol-to-the-convention-on-cybercrime-on-enhanced-co-operation-and-disclosure-of-electronic-evid (дата обращения: 15.03.2025).

Параллельно с европейской инициативой развиваются универсальные подходы в рамках ООН. Наиболее важным шагом стало принятие резолюции Генеральной Ассамблеей ООН (далее – ГА ООН) № 74/247 от 27 декабря 2019 г.[53], инициированной Россией, которая положила начало разработке всеобъемлющей универсальной Конвенции ООН «Противодействие использованию информационно-коммуникационных технологий в преступных целях» по противодействию киберпреступности. В 2021 г. был утвержден план и порядок дальнейшей работы Специального комитета по выработке такого международного документа[54]. В его деятельности активное участие принимают представители различных регионов, включая страны СНГ, Азии, Африки и Латинской Америки. Концептуальные споры в рамках этого процесса касаются, в частности, определения состава киберпреступлений, допустимого объема карательной юрисдикции, а также процедур трансграничного доступа к данным[55].

24 декабря 2024 г. Генеральная Ассамблея ООН утвердила проект Конвенции Организации Объединенных Наций против киберпреступности (далее – Конвенция ООН против киберпреступности), что ознаменовало важный этап в развитии международного права в сфере цифровой безопасности[56].

Пожалуй, инициатива Российской Федерации о создании глобального договора в целях противодействия киберпреступности является некой попыткой преодолеть недостатки существующей международно-правовой базы, основой которой остается Будапештская конвенция 2001 года. Безусловно, критика Российской Федерации этой конвенции носит не только политический, но и сугубо

---

[53] Резолюция Генеральной Ассамблеи ООН A/RES/74/247 от 27 декабря 2019 г. // Официальный сайт ООН. URL: https://docs.un.org/ru/A/RES/74/247 (дата обращения: 15.03.2025).

[54] Резолюция Генеральной Ассамблеи ООН A/RES/75/282 от 26 мая 2021 г. // Официальный сайт ООН. URL: https://docs.un.org/ru/A/RES/75/282 (дата обращения: 15.03.2025).

[55] Доклад Генерального секретаря ООН от 30 июля 2019 г. в соответствии с Резолюцией Генеральной Ассамблеи ООН A/RES/73/187 от 17 декабря 2018 г., озаглавленной «Противодействие использованию информационно-коммуникационных технологий в преступных целях» // Официальный сайт ООН. URL: https://docs.un.org/ru/A/74/130 (дата обращения: 15.03.2025).

[56] Резолюция Генеральной Ассамблеи ООН A/RES/79/243 от 24 декабря 2024 г. // Официальный сайт ООН. URL: https://docs.un.org/ru/A/RES/79/243 (дата обращения: 15.03.2025).

правовой характер, что подтверждается проведенным анализом конкретных положений этого документа.

Ввиду частого использования вредоносных программ для трансграничесих кибератак, эффективность уголовной ответственности напрямую зависит от возможностей международного сотрудничества.

Прежде всего, преамбула и ст. 39 Будапештской конвенции 2001 г. закрепляет необходимость соблюдения прав человека и основных свобод, включая право на защиту персональных данных. Но государственный суверенитет явно не является системообразующим началом. В российской версии все иначе: преамбула и ст. 4 проекта Конвенции ООН против киберпреступности подчеркивают верховенство принципов Устава ООН, включая уважение суверенитета, невмешательство, территориальную целостность и недопустимость политического давления. В международных отношениях, настоящий подход является более реалистичный и государственно-центричный.

Любое сотрудничество по запросу информации осуществляется исключительно на основании официального межгосударственного запроса, согласованного в рамках существующих двусторонних и многосторонних механизмов. Соответственно, прямой доступ к данным на территории другого государства без его предварительного уведомления или согласия категорически исключается. Именно это правило, закреплено в ст. 40 Конвенции ООН против кибепреступности, имеет особое значение для сохранения государственного суверенитета.

Серьезную критику вызвало положение, закрепленное в ст. 32 Будапештской конвенции 2001 г., которая допускает возможность получения трансграничного доступа к хранящимся данным без разрешения соответствующего государства в ограниченных случаях (например, если владелец данных дал согласие или если данные являются «публичными»), так как оно открывает возможность фактического обхода национального суверенитета и способствует одностороннему доступу к информации. Это напрямую связано с темой настоящего исследования, так как удаленный доступ к компьютерным системам часто осуществляется с

использованием «троянов» и «бэкдоров», является классическим способом применения вредоносного программного обеспечения для трансграничных атак.

Уголовно наказуемые деяния, закрепленные в Будапештской конвенции 2001 г. и предусмотренные в Конвенции ООН против киберпреступности, имеют содержательные расхождения, а именно: в ст. 2 Будапештской конвенции 2001 г. закрепляется обязанность государств криминализировать «умышленный несанкционированный доступ к любой части компьютерной системы». Здесь акцент сделан на защите целостности компьютерных систем как таковых, без учета контекста, в котором такой доступ осуществляется. Сама формулировка универсальна и технически нейтральна, направлена на пресечение любого доступа без разрешения.

В Конвенции ООН против киберпреступности аналогичный состав преступления также указан, однако с дополнительными оговорками. В ст. 7 Конвенции ООН против киберпреступности устанавливается запрет несанкционированного доступа к ИКТ-системам, но при этом подчеркивается необходимость учета последствий таких действий для национальной безопасности, общественного порядка и интересов государства. Таким образом, деяние оценивается не только как технический факт, но и через призму его возможного политического, экономического или идеологического воздействия (общественно опасные последствия).

Надо указать и на то, что на пути к появлению единого международного документа по противодействию киберпреступности активно развивались механизмы международного сотрудничества на региональном уровне.

В частности, 16 июня 2009 г. Шанхайская организация сотрудничества приняла Соглашение о сотрудничестве в области обеспечения международной информационной безопасности (далее – Соглашение ШОС 2009 г.), которое позволяет выделить ключевые аспекты, связанные с уголовной ответственностью за действия с вредоносными программами в контексте международных стандартов противодействия киберпреступности.

Соглашение ШОС 2009 г. определяет международную информационную безопасность как состояние международных отношений, исключающее нарушение мировой стабильности и создание угроз безопасности государств в информационном пространстве[57]. В этом контексте вредоносные программы рассматриваются как инструмент информационной преступности, которая определяется как использование информационных ресурсов или воздействие на них в противоправных целях[58]. Угрозы, связанные с вредоносными программами, подпадают под действие ст. 3 Соглашения ШОС 2009 г., где одним из основных направлений сотрудничества является противодействие информационной преступности. Это включает разработку совместных мер по ограничению распространения информационного оружия, к которому могут быть отнесены вредоносные программы, используемые для дестабилизации критически важных инфраструктур (п. 3 ст. 3).

Важно отметить, что Соглашение ШОС 2009 г. акцентирует необходимость совершенствования международно-правовой базы для борьбы с киберпреступностью (п. 12 ст. 3), что согласуется с позициями ученых, подчеркивающих важность гармонизации национальных законодательств в этой области. Соглашение ШОС 2009 г., таким образом, пытается частично устранить эти пробелы через региональное сотрудничество.

По справедливому мнению отдельных специалистов, в части криминализации киберпреступлений очевидно сходство подходов ШОС и СЕ, но ШОС делает больший акцент на защите государственного суверенитета в информационной сфере[59].

---

[57] Соглашение между правительствами государств – членов ШОС о сотрудничестве в области обеспечения информационной безопасности 2009 г. (Приложение 1, с. 10) // Официальный сайт ШОС. URL: https://ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreementRussian (дата обращения: 13.02.2025).

[58] См.: Соглашение между правительствами государств – членов ШОС о сотрудничестве в области обеспечения информационной безопасности 2009 г. (Приложение 1, с. 10).

[59] См.: Кириленко В.П., Алексеев Г.В. Гармонизация российского уголовного законодательства о противодействии киберпреступности с правовыми стандартами Совета Европы // Всероссийский криминологический журнал. 2020. № 6. С. 898–913.

В Приложении 1 Соглашения ШОС 2009 г. дается определение «информационного оружия», которое может включать вредоносные программы, используемые для дестабилизации общества или принуждения государства. Это созвучно с исследованиями К.К. Колина, который рассматривает вредоносные программы как инструмент гибридных войн, требующий особого правового регулирования[60]. Однако в отличие от западных подходов, где акцент делается на защите частных лиц (например, Директива ЕС NIS), Соглашение ШОС 2009 г. фокусируется на защите государственных интересов и критически важных инфраструктур (п. 8 ст. 3).

Таким образом, Соглашение ШОС 2009 г. представляет собой важный региональный инструмент, дополняющий международные подходы криминализации борьбы с киберпреступностью, включая действия с вредоносными программами. Его положения, хотя и не содержат прямых норм об уголовной ответственности, создают рамки для гармонизации национальных законодательств государств – участников в этой сфере.

В рамках СНГ еще в 2001 г. было подписано Соглашение о сотрудничестве государств в борьбе с преступлениями в сфере компьютерной информации (далее – Соглашение 2001 г.)[61], которое стало первым многосторонним документом, направленным на регулирование вопросов киберпреступности.

Этот документ был принят в период, когда законодательство большинства стран СНГ еще не содержало полноценных механизмов противодействия киберпреступности. Соглашений 2001 г. заложило основы сотрудничества правоохранительных органов в борьбе с такими деяниями. Однако его положения носили достаточно общий характер и не учитывали многих аспектов, которые стали актуальными в последующие годы. В документе отсутствовали четкие определения ключевых понятий, таких как «вредоносная программа» или

---

[60] См.: Collins S., McCombie S. Stuxnet: the emergence of a new cyber weapon and its implications // Journal of Policing, Intelligence and Counter Terrorism. 2012. Vol. 7. No. 1. P. 80–91. https://doi.org/10.1080/18335330.2012.65319.

[61] Соглашение о сотрудничестве государств в борьбе с преступлениями в сфере компьютерной информации от 1 июня 2001 г. // Законодательство стран СНГ. URL: https://base.garant.ru/12123778/ (дата обращения: 21.03.2025).

«компьютерная система», что создавало трудности при унификации правоприменения в разных странах. Кроме того, перечень уголовно наказуемых деяний был ограничен и не охватывал многие современные формы киберпреступлений. Механизмы международного сотрудничества, предусмотренные Соглашением 2001 г., также были прописаны в самом общем виде, без детализации процедур взаимодействия правоохранительных органов[62].

В последующем, в связи с бурным развитием информационных технологий, появлением новых видов киберугроз, а также имеющихся недочетов Соглашение 2001 г. утратило силу[63]. Как отмечают исследователи, Соглашение 2001 г. нуждалось в переосмыслении[64].

Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий от 28 сентября 2018 г. (далее – Соглашение 2018 г.)[65] пришло на смену устаревшему документу и ознаменовало новый этап в развитии правовых основ противодействия киберпреступности в регионе СНГ. Этот документ был принят в условиях качественного изменения характера киберугроз, когда преступления в информационной сфере стали более изощренными, масштабными и трансграничными.

В отличие от своего предшественника, Соглашение 2018 г. содержит детальные определения ключевых понятий, таких как «вредоносная программа», «информационные технологии» и «несанкционированный доступ», что способствует единообразному пониманию этих терминов в правоприменительной

---

[62] См.: Мороз Н. О. Актуальные вопросы международного сотрудничества в борьбе с преступностью в сфере высоких технологий в рамках СНГ // Международное уголовное право и международная юстиция. 2016. № 3. С. 13.

[63] См.: Соглашение между правительствами государств – членов ШОС о сотрудничестве в области обеспечения информационной безопасности 2009 г.

[64] См.: Архипова Е. А., Додонов В. Н. Международно-правовые проблемы сотрудничества при выявлении, расследовании и предупреждении преступлений, совершенных с использованием информационно-телекоммуникационных сетей и в сфере компьютерной информации // Московский журнал международного права. 2020. № 2. С. 85.

[65] Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий 2018 г. // Законодательство стран СНГ. URL: https://base.spinform.ru/show_doc.fwx?rgn=110821 (дата обращения: 13.02.2025).

практике разных стран. Значительно расширен перечень уголовно наказуемых деяний: теперь в него включены не только традиционные компьютерные преступления, но и такие современные формы противоправных действий, как распространение детской порнографии (п. «д» ст. 3), экстремистских материалов (п. «з» ст. 3), а также нарушения авторских прав в цифровой среде (п. «ж» ст. 3).

По мнению А.И. Мысиной, Соглашение 2018 г. содержит оптимальное количество составов преступлений в сфере информационных технологий, которые необходимы для осуществления эффективного сотрудничества[66].

Особое внимание уделено механизмам международного сотрудничества: детально прописаны процедуры направления и исполнения запросов, условия конфиденциальности информации, основания для отказа в правовой помощи.

Другим масштабным международным документом в рамках противодействия киберпреступности можно рассматривать Конвенцию о борьбе с преступлениями в сфере информационных технологий, которая была подписана в 2010 г. под эгидой Лиги арабских государств (далее – Конвенция ЛАГ 2010 г.)[67]. Конвенция ЛАГ 2010 г. демонстрирует системный подход к формированию понятийного аппарата и определению перечня киберпреступлений, что соответствует современным тенденциям международно-правового регулирования в данной области. Как справедливо отмечает А.И. Мысина, ст. 2 Конвенции ЛАГ 2010 г. устанавливает четкие дефиниции ключевых терминов, включая «информационные технологии», «данные», «информационная система» и другие, что создает необходимую терминологическую основу для эффективного международного сотрудничества. Особого внимания заслуживает определение информационных технологий как «совокупности средств, методов и процессов сбора, обработки, накопления, хранения, поиска и передачи информации с

---

[66] См.: Мысина А. И. Международно-правовое регулирование сотрудничества государств по противодействию преступлениям в сфере информационных технологий: дис. ... канд. юрид. наук. М., 2021. С. 59.

[67] Конвенция Лиги арабских государств о борьбе с преступлениями в сфере информационных технологий 2010 г. URL: https://www.asianlaws.org/gcld/cyberlawdb/GCC/Arab%20Convention%20on%20Combating%20Information%20Technology%200ffences.pdf. (дата обращения: 13.02.2025).

использованием компьютерной и телекоммуникационной техники»[68] (ст. 2). Такой подход, способствует унификации правового понимания базовых категорий в регионе.

Перечень составов преступлений, закрепленный в Конвенции ЛАГ 2010 г., отличается значительной детализацией и широтой охвата. Как отмечает А.И. Мысина, документ включает не только «классические» киберпреступления (несанкционированный доступ, перехват данных, воздействие на целостность информации), но и специальные составы, отражающие региональную специфику и современные вызовы[69]. В частности, ст. 15 Конвенции ЛАГ 2010 г., посвященная кибертерроризму, представляет собой пример адаптации международно-правовых моделей к местным условиям безопасности. При этом важно отметить, что перечень преступлений в Конвенции ЛАГ 2010 г. в целом соответствует подходу, закрепленному в Будапештской конвенции 2001 г., хотя и содержит дополнительные составы, связанные с защитой культурных и религиозных ценностей.

По сравнению с другими региональными инструментами, Конвенцию ЛАГ 2010 г. является удачным пример, которая сочетает, как в себе общепризнанные международно-правовые ориентири и региональную специфику. Можно отметить, что подобная модель может быть полезна для дальнейшего развития международно-правового регулирования в сфере противодействия киберпреступности, особенно в условиях необходимости учета культурных и правовых особенностей разных регионов мира.

Конвенция Африканского союза о кибербезопасности и защите персональных данных 2014 г. (далее – Конвенция АС 2014 г.)[70], известная также как Малабская конвенция, представляет собой комплексный международно-правовой инструмент, направленный на гармонизацию законодательств

---

[68] Мысина А. И. Указ. соч. С. 52–53.
[69] См.: Мысина А. И. Указ. соч. С. 56–57.
[70] Конвенция Африканского союза о кибербезопасности и защите персональных данных 2014 г. // Официальный сайт Африканского союза. URL: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection (дата обращения: 21.02.2025).

африканских государств в сфере противодействия киберпреступности и защиты персональных данных. В ст. 1 Конвенции АС 2014 г. содержится детализированный понятийный аппарат, включающий такие ключевые категории, как «детская порнография», «компьютерная система», «критическая инфраструктура», «обработка персональных данных» и другие. Настоящая терминологическая конкретизация демонстрирует достижение единообразия в правоприменительной практике.

Особого внимания заслуживает ст. 30 Конвенции АС 2014 г., которая содержит специальные положения о преступлениях экстремистской направленности, включая отрицание или оправдание геноцида посредством компьютерных систем. Важной новацией является положение п. “b” ч. 1 ст. 30, которое предписывает рассматривать использование информационно-коммуникационных технологий при совершении терроризма и отмывания денег в качестве отягчающего обстоятельства[71].

Важным аспектом Конвенции АС 2014 г. является ее ориентированность на создание комплексной системы защиты персональных данных. Как отмечает Л.Ю. Фомина, документ закрепляет базовые принципы обработки данных, включая требование согласия, законности и конфиденциальности, что соответствует современным международным стандартам[72].

Таким образом, Конвенция АС 2014 г. представляет собой значительный шаг в развитии регионального сотрудничества по противодействию киберпреступности. Как подчеркивает Е. В. Дробот, дальнейшее развитие конвенционного режима потребует принятия дополнительных нормотворческих

---

[71] См.: Русскевич Е. А. Дифференциация ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий, и проблемы их квалификации: дис. ... д-ра юрид. наук. М., 2020. С. 85.

[72] См.: Фомина Л. Ю. Международные стандарты защиты персональных данных в условиях информационного общества // Международное право. 2019. № 4. С. 52.

уточнений, учитывающих социокультурное разнообразие африканского континента[73].

В рамках объединения БРИКС противодействие киберпреступности является приоритетным направлением регионального сотрудничества. На сегодняшний день, отсутствует единый региональный международный договор в рамках данного объединения, однако, БРИКС вырабатывает совместные подходы в борьбе с киберпреступностью.

Впервые упоминание о «борьбе с киберпреступность» было в 2011 г., где необходимость сотрудничества была обозначена в декларациях саммитов.
Российская Федерация неоднократно выступала с инициативой по разработке многостороннего соглашения по противодействию с киберпреступности, но данные предложения не получили поддержки со стороны участников объединения[74].

Интерес вызывают позиции стран БРИКС, которые демонстрируют различную степень заинтересованности в этом вопросе. Например, Индия и ЮАР поддержали инициативу России о разработке соглашения, тогда как Китай и Бразилия заняли противоположную позицию, аргументируя тем, что уже существует достаточное количество механизмов[75]. Это свидетельствует о том, что даже в рамках относительно близкой на международной арене группы государств достижение консенсуса по вопросам кибербезопасности остается сложной задачей.

Однако, в рамках таких форматов, как встречи представителей по безопасности, министров и Рабочей группы по сотрудничеству страны БРИКС уделяют значительное внимание. В 2016 г. был принят План совместных действий стран БРИКС в области ИКТ, который, однако, не предусматривает конкретных

---

[73] См.: Дробот Е. В. Новые приоритеты национальной безопасности стран Африки в условиях нарушения глобальных цепочек создания стоимости // Экономические отношения. 2022. Т. 12. № 2. С. 299.
[74] См.: Муратшина К. Г. К вопросу о сотрудничестве в области информационной безопасности в рамках БРИКС // Гуманитарное знание и искусственный интеллект: стратегии и инновации: 4-й молодежный конвент УрФУ: материалы международной конференции 26 марта 2020 г. Екатеринбург: Изд-во Урал. ун та, 2020. С. 617.
[75] См.: Муратшина К. Г. Указ. соч. С. 617.

мер по противодействию вредоносным программам или установлению уголовной ответственности за такие действия[76].

Согласно документу, особое внимание заслуживает позиция Российской Федерации, которая выступает с инициативой разработки международно-правого документа в целях создания правовых рамок для сотрудничества в сфере противодействия киберпрестпуности[77]. Безусловно, настоящая инициатива соответствует Доктрине информационной безопасности РФ, где подчеркивается необходимость защиты от внутренних и внешних информационных угроз[78].

25 октября 2025 г. стал исторической вехой в развитии международного сотрудничества по противодействию киберпреступности. В этот день была официально открыта для подписания Конвенция ООН против киберпреступности[79], признанная создать глобальную правовую основу для борьбы с киберпреступностью. В первый же день процедуры свои подписи под документом поставили 65 государств из различных регионов[80].

В этом контексте особенно важным представляется проведение сравнительно-правового анализа уголовного законодательства Российской Федерации и Кыргызской Республики в целях выявления положений Конвенции ООН против киберпреступности, которые могли бы быть полезны для совершенствования национальных норм.

---

[76] См.: Принят план совместных действий стран БРИКС в области ИКТ // Министерство цифрового развития, связи и массовых коммуникаций РФ. URL: https://digital.gov.ru/news/prinyat-plan-sovmestnyh-dejstvij-stran-briks-v-oblasti-ikt (дата обращения 25.03.2025).

[77] Резолюция Генеральной Ассамблеи ООН от 24 декабря 2024 г. // Официальный сайт ООН. URL: https://docs.un.org/ru/A/RES/79/243 (дата обращения: 25.03.2025).

[78] Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СЗ РФ. 2016. № 50. Ст. 7074.

[79] Конвенция Организации Объединенных Наций против киберпреступности; укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям, 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 (дата обращения: 20.02.2026).

[80] См.: Шестьдесят пять стран подписали Конвенцию ООН против киберпреступности. URL: https://news.un.org/ru/story/2025/10/1466671 (дата обращения: 25.12.2025).

В целом уголовное законодательство Российской Федерации и Кыргызской Республики воплощает основные идеи Конвенции ООН против киберпреступности, однако между ними существует ряд фундаментальных различий. В рамках исследования ключевое значение имеют ст. 7–11 Конвенции ООН против киберпреступности.

Так, ст. 7 Конвенции ООН против киберпреступности предусматривает криминализацию самого факта неправомерного доступа, тогда как ст. 272 УК РФ и ст. 319 УК КР сконструированы как материальные составы. По справедливому замечанию Д.В. Пучкова, ст. 272 УК РФ оставляет безнаказанным «взлом» как таковой без наступления вредоносных последствий[81].

В Российской Федерации воспроизведены положения ст. 8 Конвенции ООН против киберпреступности – «незаконный перехват», осуществляемый с помощью технических средств перехват непубличных передач данных, полностью реализовано в ст. 138 УК РФ «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений», которая охватывает перехват электронных данных, которые должны быть защищены от технического вмешательства. В Кыргызской Республике, норма, криминализующая акт технического перехвата электронных данных, предусмотрена ст. 193 УК КР «Нарушение тайны переписки».

Если рассматривать, ст. 9 и 10 Конвенции ООН против киберпреступности, то в этой части законодательства обеих стран содержит сходные по содержанию нормы, охватывающие соответствующие деяния. В Российской Федерации уголовная ответственность за неправомерное воздействие на электронные данные предусмотрена ст. 272 и 273 УК РФ, а неправомерное воздействие на информационно-коммуникационную систему критической значимости предусмотрено в ст. 274^1 УК РФ.

---

[81] См.: Пучков Д. В. Глобальная политика в сфере уголовно-правовой защиты общества от киберпреступности: международные обязательства Российской Федерации при ратификации Конвенции ООН (2024) // Правопорядок: история, теория, практика. 2025. № 3 (46). С. 150.

В Кыргызской Республике аналогичные деяния предусмотрены ст. 319 УК КР и ст. 320 УК КР (в части уничтожения, блокирования, изменения информации), но ключевое значение имеет наличие самостоятельной ст. 321 УК КР («Киберсаботаж»), которая прямо устанавливает ответственность за действия, совершенные «с намерением помешать функционированию программных продуктов или телекоммуникационных систем, а также вывод из строя программных продуктов, оборудования». Данная норма практически текстуально воспроизводит норму ст. 10 Конвенции ООН против киберпреступности о «серьезном препятствовании функционированию системы». Наличие ст. 321 УК КР позволяет более точно квалифицировать атаки типа DoS/DDoS и иные формы воздействия на систему, даже если они совершены без использования традиционных вредоносных программ. Российское законодательство, увязывая ответственность за воздействие на систему преимущественно с использованием вредоносных программ (ст. 274^1 УК РФ), является в этом аспекте более узким.

Однако наиболее острым и системным пробелом является имплементация ст. 11 Конвенции ООН против киберпреступности.

Во-первых, пп. «а» п. 1 ст. 11 Конвенции ООН против киберпреступности закрепляет более расширенный перечень действий объективной стороны преступления, т.е. помимо создания, распространения и использования, которые предусмотрены в ст. 273 УК РФ и ст. 320 УК КР, предполагается криминализация также получения, производства, продажи, приобретения для использования, ввоза и предоставления иным способом.

Во-вторых, пп. «в» п. 1 ст. 11 Конвенции ООН против киберпреступности прямо устанавливает необходимость от государств-участников признать в качестве уголовно наказуемого деяния владение (хранение) объектами, указанными в пп. (i) и (ii), с намерением их использования для совершения киберпреступлений, что также не предусмотрено уголовным законодательством обеих стран.

Конвенция ООН против киберпреступности содержит подход, устанавливающий ответственность за оборот не только устройств и программ, но и «пароля, реквизитов доступа, электронной подписи или аналогичных данных»,

предназначенных для совершения преступлений согласно ст. 7–10 Конвенции ООН.

Буквальное толкование ст. 273 УК РФ не позволяет распространить ее действие на оборот паролей и реквизитов доступа и т.д. С одной стороны, отнесение паролей, реквизитов доступа и электронной подписи к категории компьютерной информации, как это следует из примечания к ст. 272 УК РФ и разъяснений, содержащихся в п. 3 постановления Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37[82], создает иллюзию полной имплементации международных стандартов. Действительно, согласно легальному определению компьютерной информацией признаются сведения, представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. Пароль, существующий в цифровом виде на машинном носителе или передаваемый по телекоммуникационным каналам, безусловно, подпадает под данное определение, что позволяет рассматривать его в качестве предмета преступления, предусмотренного ст. 272 УК РФ. С другой стороны, подобный технико-юридический подход, не учитывает различий в конструкции составов преступлений, несмотря на отождествляющую форму существования информации с ее уголовно-правовым значением.

Введение в 2025 г. ст. 274[5] УК РФ существенно меняет оценку российского законодательства, в связи с тем, что данная новелла максимально полностью приближена к норме пп. “a” (ii) п. 1 ст. 11 Конвенции ООН против киберпреступности о необходимости криминализировать незаконный оборот идентификаторов доступа к информационным ресурсам.

Сопоставление уголовного законодательства Кыргызской Республики со ст. 11 Конвенции ООН против киберпреступности показывает иную картину. В части первого блока (пп. “a” (i) п. 1 ст. 11), касающегося вредоносных программ, норма

---

[82] 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». URL: https://www.consultant.ru/document/cons_doc_LAW_434573/ (дата обращения: 15.02.2026).

частично охватывается ст. 320 УК КР. Однако второй, не менее важный блок (пп. “a” (ii) п. 1), устанавливающий криминализацию оборота паролей, реквизитов доступа и электронных подписей, в УК КР отсутствует полностью.

Пожалуй, одна из самых важных оговорок Конвенции ООН против киберпреступлений содержится в п. 2 ст. 11, где прямо определено, что положения данной статьи не должны толковаться как требующие привлечения к уголовной ответственности за деяния, совершенные в разрешенных целях, в частности, для проведения испытаний или защиты информационно-коммуникационных систем. Другими словами, Конвенция ООН против киберпреступности проводит четкую границу между преступным и легитимными инструментами, используемыми специалистами по кибербезопасности, исследователями и разработчиками в профессиональных целях. Данное положение является значимым, так как без него криминализация оборота вредоносных программ может парализовать деятельность добросовестность участиноков рынка в цифровой среде.

Таким образом, следует сделать вывод, что ст. 273 УК РФ в целом коррелирует с положениями пп. “a” (i) п. 1 ст. 11 Конвенции ООН против киберпреступности. В целях совершенствования ст. 273 УК РФ представляется целесообразным расширить объективную сторону состава преступления, дополнив диспозицию такими действиями, как приобретение, ввоз на территорию Российской Федерации и хранение вредоносных компьютерных программ аналогично подходу, заложенному в ст. 11 Конвенции ООН против киберпреступности, а также закрепить оговорку, исключающую ответственность за правомерные (санкционированные владельцем компьютерной системы) действия специалистов по кибербезопасности и исследователей, что будет полностью отражать подход, закрепленный в п. 2 ст. 11 Конвенции ООН против киберпреступности.

Прогрессивным шагом российского законодателя несомненно следует признать введение в 2025 г. ст. 274^5 УК РФ. Данная новелла впервые криминализирует оборот средств доступа к компьютерной информации, включая пароли, реквизиты доступа и электронную подпись. Ранее подобные деяния,

являющиеся неотъемлемым элементом подготовки и совершения преступлений с использованием вредоносных программ, либо оставались вне поля действия уголовного закона, либо требовали сложной и не всегда успешной квалификации. Таким образом, имплементация пп. “a” (ii) п. 1 ст. 11 Конвенции ООН против киберпреступности в российское законодательство позволяет рассматривать как положительный пример использования международного опыта при совершенствовании национального законодательства в части противодействия обороту средств доступа, предназначенных для совершения, в том числе преступлений, связанных с вредоносными программами.

В то же время анализ международных норм в аспекте оценки состояния уголовного законодательства Кыргызской Республики о компьютерных преступлениях выявил несколько иную ситуацию. В ст. 320 УК КР криминализованы создание, использование и распространение вредоносных программ, что по своему содержанию практически идентично российской ст. 273 УК РФ и, следовательно, так же не в полной мере охватывает весь перечень действий, закрепленных в пп. “a” (i) п. 1 ст. 11 Конвенции. Важно отметить, что в ст. 320 УК КР аналогично ст. 273 УК РФ отсутствуют положения, закрепленные в п. 2, 3 ст. 11 Конвенции ООН против кибепреступности.

Однако наиболее существенный пробел выявлен в отношении второго блока положений. В УК КР полностью отсутствует норма, аналогичная новой российской ст. 274^5 УК РФ, которая бы устанавливала ответственность за оборот паролей, реквизитов доступа и электронных подписей. Следовательно, это означает, что уголовное законодательство не консолидируется с положением пп. “a” (ii) п. 1 ст. 11 Конвенции ООН против киберпреступности, оставляя безнаказанным оборот сетевых идентификаторов пользователей, предназначенных для совершения киберпреступлений.

На данный момент отсутствует какая-либо информация в открытых источниках о рассмотрении возможности присоединения Кыргызской Республики к недавно открытой конвенции ООН против киберпреступности.

Поскольку документ только начал путь к вступлению в силу и круг его участников еще не сформирован, публичная позиция официальных органов страны по данному вопросу пока не обозначена. Вместе с тем с учетом отчетливого вектора уголовной политики Кыргызстана на усиление мер в сфере кибербезопасности и ужесточение борьбы с цифровыми преступлениями присоединение к данной Конвенции ООН против киберпреступности в перспективе представлялось бы вполне целесообразным и логичным шагом. Это позволило бы стране своевременно включиться в формирующуюся международную архитектуру противодействия киберугрозам и обеспечить гармонизацию национального законодательства с новыми глобальными ориентирами в указанной области.

§ 3. Ответственность за действия с вредоносными компьютерными программами по законодательству стран Содружества Независимых Государств

Выделение самостоятельного параграфа, посвященного краткому сравнительно-правовому анализу уголовного законодательства об ответственности за преступные действия с вредоносными компьютерными программами в рамках СНГ, преимущественно было продиктовано той целью, чтобы показать те основные подходы (не всегда совпадающие), которые сложились за прошедшие годы в части криминализации и пенализации. Расхожее представление о малых или даже ничтожных отличиях в уголовном законодательстве стран Содружества уже не имеет под собой оснований. За прошедшие 30 лет уголовные кодексы стран менялись многократно, поскольку не оставалась неизменной уголовная политика государств, доктрина, социальные и экономические условия. В результате правовое пространство Содружества хотя и имеет общие корни в советском наследии, но уже далеко не монолитно во многих аспектах. Конечно же, степень «удаления» друг от друга существенно разнится в зависимости от конкретного предмета правового регулирования. Однако это не меняет общего вывода о том, что в рамках Содружества по многим вопросам уголовно-правовой охраны – и уголовная

ответственность за действия с вредоносными компьютерными программами здесь не исключение – мы имеем не унифицированное решение, а множество таких решений, имеющих иногда довольно принципиальные отличия.

В целях репрезентативности последующего анализа ниже приведены статьи уголовного законодательства стран Содружества, предусматривающие ответственность за действия с вредоносными компьютерными программами, по состоянию на 2025 г.

Уголовный кодекс Российской Федерации	**Статья 273. Создание, использование и распространение вредоносных компьютерных программ** 1. Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, – наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев. 2. Деяния, предусмотренные частью первой настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно причинившие крупный ущерб или совершенные из корыстной заинтересованности, – наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, либо лишением свободы на срок до пяти лет со штрафом в размере от ста тысяч до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от двух до трех лет или без такового и с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового. 3. Деяния, предусмотренные частями первой или второй настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, – наказываются лишением свободы на срок до семи лет
Уголовный Кодекс Кыргызской Республики	**Статья 320. Создание вредоносных программных продуктов** 1. Создание с целью использования либо распространения программного продукта или внесение изменений в существующие программные продукты, заведомо предназначенные для осуществления несанкционированного доступа и копирования, уничтожения, блокирования, изменения компьютерной информации и электронных документов или нейтрализации средств защиты информации, нарушения работы информационных систем или сети электросвязи, а равно

	умышленное использование и распространение таких программных продуктов, повлекших причинение значительного ущерба или иного значительного вреда, – наказываются общественными работами от сорока до ста часов или лишением права занимать определенные должности либо заниматься определенной деятельностью на срок до двух лет, или исправительными работами на срок от двух месяцев до одного года, или штрафом от 200 до 500 расчетных показателей. 2. То же деяние, совершенное: 1) группой лиц по предварительному сговору; 2) с причинением по неосторожности крупного ущерба или иного тяжкого вреда; 3) в отношении информационных систем и сетей электросвязи, относящихся к критической информационной инфраструктуре, – наказывается штрафом от 500 до 1000 расчетных показателей или лишением свободы на срок до пяти лет с лишением права занимать определенные должности либо заниматься определенной деятельностью на срок до двух лет или без такового
Уголовный кодекс Республики Казахстан[83]	**Статья 210. Создание, использование или распространение вредоносных компьютерных программ и программных продуктов** 1. Создание компьютерной программы, программного продукта или внесение изменений в существующую программу или программный продукт с целью неправомерного уничтожения, блокирования, модификации, копирования, использования информации, хранящейся на электронном носителе, содержащейся в информационной системе или передаваемой по сетям телекоммуникаций, нарушения работы компьютера, абонентского устройства, компьютерной программы, информационной системы или сетей телекоммуникаций, а равно умышленные использование и (или) распространение такой программы или программного продукта – наказываются штрафом в размере до трех тысяч месячных расчетных показателей либо исправительными работами в том же размере, либо привлечением к общественным работам на срок до восьмисот часов, либо ограничением свободы на срок до трех лет, либо лишением свободы на тот же срок, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового. 2. Те же деяния, совершенные: 1) группой лиц по предварительному сговору; 2) лицом с использованием своего служебного положения; 3) в отношении критически важных объектов информационно-коммуникационной инфраструктуры, – наказываются ограничением свободы на срок от трех до семи лет либо лишением свободы на тот же срок, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового. 3. Деяния, предусмотренные частями первой или второй настоящей статьи:

[83] Уголовный кодекс Республики Казахстан от 3 июля 2014 г. № 226-V. (по сост. на 2 мая 2025 г.) [Электронный ресурс]. URL: https://online.zakon.kz/Document/?doc_id=31575252 (дата обращения: 10.05.2025).

	1) совершенные преступной группой; 2) повлекшие тяжкие последствия, – наказываются лишением свободы на срок от пяти до десяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет или без такового.
Уголовный кодекс Таджикистана[84]	**Статья 303. Разработка, использование и распространение вредоносных программ** 1. Разработка компьютерных программ или внесение изменений в существующие программы с целью несанкционированного уничтожения, блокирования, модификации или копирования информации, хранящейся в компьютерной системе, сети или на машинных носителях, а также разработка специальных вирусных программ, заведомое их использование или распространение носителей с такими программами, – наказывается штрафом в размере от трехсот до пятисот показателей для расчетов либо ограничением свободы на срок до двух лет. 2. То же деяние, повлекшее по неосторожности тяжкие последствия, – наказывается штрафом в размере от пятисот до одной тысячи показателей для расчетов либо лишением свободы до трех лет
Уголовный кодекс Республики Беларусь[85]	**Статья 354. Разработка, использование, распространение либо сбыт вредоносных компьютерных программ или специальных программных или аппаратных средств** 1. Разработка, использование, распространение либо сбыт компьютерной программы или специального программного или аппаратного средства, заведомо предназначенных для нарушения системы защиты, несанкционированного доступа к компьютерной системе, сети или машинному носителю, несанкционированного уничтожения, блокирования, модификации компьютерной информации или неправомерного завладения компьютерной информацией либо нарушения работы компьютерной системы, сети или машинного носителя, – наказываются штрафом, или арестом, или ограничением свободы на срок до трех лет, или лишением свободы на тот же срок. 2. Те же действия, совершенные группой лиц по предварительному сговору, – наказываются штрафом, или арестом, или ограничением свободы на срок до пяти лет, или лишением свободы на тот же срок с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения. 3. Действия, предусмотренные частями 1 или 2 настоящей статьи, повлекшие по неосторожности последствия, указанные в части 2 статьи 349 настоящего Кодекса, –

[84] Уголовный кодекс Республики Таджикистан от 21 мая 1998 г. № 574 (по сост. на 24 апреля 2025 г.) [Электронный ресурс]. URL: https://continent-online.com/Document/?doc_id=30397325 (дата обращения: 01.05.2025).

[85] Уголовный Кодекс Республики Беларусь от 19 июля1999 г. № 275-З. (по сост. на 24 апреля 2025 г.) [Электронный ресурс]. URL: https://online.zakon.kz/Document/?doc_id=30414984 (дата обращения: 01.05.2025).

	наказываются лишением свободы на срок от трех до десяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.
Уголовный Кодекс Республики Узбекистан[86]	**Статья 278-6. Создание, использование или распространение вредоносных программ** Создание компьютерных программ или внесение изменений в существующие программы с целью несанкционированного уничтожения, блокирования, модификации, копирования или перехвата информации, хранящейся или передаваемой компьютерной системе, а равно разработка специальных вирусных программ, их умышленное использование или распространение – наказывается штрафом от ста до трехсот базовых расчетных величин или ограничением свободы до двух лет либо лишением свободы до двух лет. Те же действия, совершенные: а) с причинением особо крупного ущерба; б) по предварительному сговору группой лиц; в) повторно или опасным рецидивистом; г) организованной группой или в ее интересах, – наказываются ограничением свободы от двух до трех лет либо лишением свободы от двух до трех лет.
Уголовный кодекс Республики Азербай-джан[87]	**Статья 273-1. Оборот средств, изготовленных для совершения киберпреступлений** 273-1.1. Производство устройств или компьютерных программ, основной целью изготовления или адаптации которых является совершение преступлений, предусмотренных статьями 271–273 настоящего Кодекса, их ввоз с целью совершения данных преступлений, приобретение для использования, продажа, распространение и создание других условий для их приобретения, если это причинило значительный ущерб – наказываются штрафом в размере от трех тысяч до пяти тысяч манатов или лишением свободы на срок до двух лет с лишением права занимать определенную должность или заниматься определенной деятельностью на срок до двух лет. 273-1.2. Создание, хранение или приобретение для использования паролей от компьютеров, кодов доступа или иных аналогичных данных, позволяющих получить несанкционированный доступ в компьютерную систему или какую-либо ее часть, с целью совершения преступлений, предусмотренных статьями 271–273 настоящего Кодекса, если это причинило значительный ущерб, – наказываются штрафом в размере от трех тысяч до пяти тысяч манатов или лишением свободы на срок до двух лет с лишением права занимать определенную должность или заниматься определенной деятельностью на срок до двух лет.

[86] Уголовный кодекс Республики Узбекистан (утвержден Законом Республики Узбекистан от 22 сентября 1994 г. № 2012-XII) (по сост. на 24 апреля 2025 г.) [Электронный ресурс]. URL: https://online.zakon.kz/Document/?doc_id=30421110 (дата обращения: 01.05.2025).

[87] Уголовный кодекс Азербайджанской Республики (утвержден Законом Азербайджанской Республики от 30 декабря 1999 г. № 787-IQ). (по сост. на 11 мая 2025 г.) [Электронный ресурс]. URL: https://continent-online.com/Document/?doc_id=30420353 (дата обращения: 18.05.2025).

	273-1.3. Продажа, распространение или создание других условий для приобретения паролей от компьютеров, кодов доступа или иных аналогичных данных, позволяющих получить несанкционированный доступ в компьютерную систему или какую-либо ее часть, с целью совершения преступлений, предусмотренных статьями 271–273 настоящего Кодекса – наказываются штрафом в размере от трех тысяч до пяти тысяч манатов или лишением свободы на срок до двух лет с лишением права занимать определенную должность или заниматься определенной деятельностью на срок до двух лет. 273-1.4. Деяния, предусмотренные статьями 273-1.1–273-1.3, совершенные: 273-1.4.1. повторно; 273-1.4.2. группой лиц по предварительному сговору, организованной группой или преступным сообществом (организацией); 273-1.4.3. должностным лицом с использованием своего служебного положения – наказываются штрафом в размере от пяти тысяч до восьми тысяч манатов или лишением свободы на срок от двух до четырех лет с лишением права занимать определенную должность или заниматься определенной деятельностью на срок
Уголовный кодекс Республики Армения[88]	**Статья 363. Незаконный оборот специальных программных или инструментальных средств** 1. Производство, изготовление, разработка, импорт, приобретение, хранение, перемещение, поставка или экспорт предусмотренных для доступа в компьютер, компьютерную систему или компьютерную сеть без разрешения или уничтожения, изменения, повреждения, искажения или блокирования (изоляции) компьютерного сведения, или его незаконного извлечения, или незаконного овладения им специальных программных или инструментальных средств или специальных вирусных программ в целях их использования или реализации, или реализация или использование такого программного или инструментального средства или программы – наказывается штрафом максимально в двадцатикратном размере, или общественными работами продолжительностью от восьмидесяти до ста пятидесяти часов, или лишением права занимать определенные должности или заниматься определенной деятельностью на срок от двух до пяти лет, или ограничением свободы максимально на срок два года, или краткосрочным лишением свободы максимально на срок два месяца, или лишением свободы максимально на срок два года. 2. Деяние, предусмотренное частью 1 настоящей статьи, которое: 1) совершено из корыстных побуждений; 2) совершено группой лиц по предварительному сговору; 3) совершено в целях сокрытия или облегчения совершения другого преступления или 4) повлекло по неосторожности имущественный ущерб в крупных размерах, расстройство деятельности учреждения или организации, аварию или бедствие, уничтожение, изменение, блокирование

[88] Уголовный кодекс Республики Армения от 27 мая 2021 г. № ЗР-199. (по сост. на 13 мая 2025 г.) [Электронный ресурс]. URL: https://continent-online.com/Document/?doc_id=39571894 (дата обращения: 20.05.2025).

	(изоляцию) сведения, имеющего особую ценность, или иное тяжкое последствие – наказывается штрафом от двадцатикратного до пятидесятикратного размера, или общественными работами продолжительностью от ста пятидесяти до двухсот семидесяти часов, или лишением права занимать определенные должности или заниматься определенной деятельностью на срок от трех до семи лет, или ограничением свободы на срок от одного года до трех лет, или краткосрочным лишением свободы на срок от одного до двух месяцев, или лишением свободы на срок от двух до пяти лет. 3. Деяние, предусмотренное частью 1 или 2 настоящей статьи, которое: 1) совершено преступной организацией или 2) повлекло по неосторожности имущественный ущерб в крупных размерах, расстройство деятельности учреждения или организации, аварию или бедствие, уничтожение, изменение, блокирование (изоляцию) сведения, имеющего особую ценность, или иное тяжкое последствие – наказывается лишением свободы на срок от трех до шести лет. 4. Лицо, добровольно передавшее компетентному органу программное или инструментальное средство или программу, предусмотренные частью настоящей статьи, освобождается от предусмотренной настоящей статьей уголовной ответственности. Если фактически совершенное лицом деяние содержит иной состав преступления, то оно подлежит уголовной ответственности за это преступление.
Уголовный кодекс Туркмени-стана[89]	**Статья 379. Создание, использование и распространение вредоносных программ** 1. Незаконное уничтожение охраняемой законом информации в информационной системе или проходящей через информационно-телекоммуникационную сеть, хранящейся на электронном носителе, создание компьютерных программ с целью нарушения нормальной работы компьютера, устройства абонента, компьютерных программ, системы информации или информационно-телекоммуникационной сети или производство программной продукции или внесение изменений в имеющиеся программы или в программную продукцию, их блокировка, изменение формата, копирование, а равно преднамеренное использование или распространение таких программ или программной продукции, – наказываются штрафом в размере от пятидесяти до ста размеров установленной базовой величины с лишением права занимать определенную должность или заниматься определенной деятельностью на срок до двух лет или без такового или лишением свободы на срок до трех лет с лишением права занимать определенную должность или заниматься определенной деятельностью на срок до двух лет или без такового. 2. Те же деяния, если они совершены в отношении источников национальной электронной информации, национальной информационной системы или критически важных объектов

[89] Уголовный кодекс Туркменистана от 12 июня 1997 г. № 222-I. (по сост. на 17 мая 2025 г.) [Электронный ресурс]. URL: https://continent-online.com/Document/?doc_id=31295286 (дата обращения: 25.05.2025).

	информационно-коммуникационной инфраструктуры или с использованием служебного положения, – наказываются лишением свободы на срок от трех до семи лет с лишением права занимать определенную должность или заниматься определенной деятельностью на срок до трех лет или без такового. 3. Деяния, предусмотренные частями первой и второй настоящей статьи, если они повлекли тяжкие последствия или совершены группой лиц по предварительному сговору или организованной группой, – наказываются лишением свободы на срок от пяти до десяти лет с лишением права занимать определенную должность или заниматься определенной деятельностью на срок до трех лет или без такового
Уголовный кодекс Молдовы[90]	**Статья 260. Неправомерные производство, импорт, продажа или предоставление технических средств или программных продуктов** Неправомерные производство, импорт, продажа или иные формы предоставления в пользование технических средств или программных продуктов, пароля, кода доступа или аналогичных информационных данных, обеспечивающих возможность полного или частичного доступа к информационной системе, разработанных или адаптированных для целей совершения одного из преступлений, предусмотренных статьями 237, 259, 260-1–260-3, 2605–2607, – наказываются штрафом в размере от 850 до 1350 условных единиц или лишением свободы на срок от 2 до 5 лет, а в случае юридического лица – штрафом в размере от 4000 до 7000 условных единиц с лишением права заниматься определенной деятельностью или ликвидацией предприятия

Как показывает изучение уголовного законодательства стран Содружества, установление ответственности за деяния, связанные с вредоносными компьютерными программами, получило нормативное закрепление повсеместно, исключений в этом отношении обнаружено не было. При этом наблюдаются сходства и значительные различия как в содержании криминообразующих признаков, так и в подходах к пенализации.

Основной непосредственный объект исследуемого преступления по уголовному законодательству стран Содружества традиционно определяется как общественные отношения в сфере безопасного обращения с компьютерной информацией. Это включает защиту целостности, конфиденциальности и доступности данных, а также стабильность работы информационных систем.

[90] Уголовный кодекс Республики Молдова от 18 апреля 2002 г. № 985-XV. (по сост. на 17 мая 2025 г.) [Электронный ресурс]. URL: https://continent-online.com/Document/?doc_id=30394923 (дата обращения: 25.05.2025).

В большинстве уголовных кодексов основной акцент делается именно на защиту информации и программного обеспечения. Например, ст. 273 УК РФ формулирует состав преступления как создание, использование или распространение вредоносных программ, *заведомо предназначенных* для уничтожения, блокирования, модификации или копирования компьютерной информации. Аналогичная формулировка содержится в ст. 303 УК Таджикистана, где объектом преступления выступает именно информационная безопасность.

В этих случаях законодатель концентрируется на защите цифровых данных и программных алгоритмов, не акцентируя внимание на физических носителях или сетевой инфраструктуре. Такой подход характерен для стран, где уголовное право в сфере киберпреступлений развивалось в рамках традиционных представлений о компьютерных преступлениях, унаследованных еще от советской правовой доктрины.

Однако при детальном рассмотрении норм различных государств становится очевидным, что законодатели некоторых стран расширяют этот объект, включая в него не только программное обеспечение и данные, но и аппаратные средства, телекоммуникационные сети.

Например, в ст. 354 УК Беларуси и ст. 210 УК Казахстана имеется прямое упоминание в диспозиции статьи про аппаратные средства, в ст. 320 УК КР – про сети электросвязи, т.е. подразумевается повреждение серверов, маршрутизаторов и другого сетевого оборудования.

Сравнительно-правовой анализ дополнительного непосредственного объекта преступлений, связанных с вредоносными компьютерными программами в уголовном законодательстве стран Содружества, позволяет глубже осмыслить направленность на охраняемые уголовным законом ценности, выходящие за пределы информационной безопасности как основного объекта. Несмотря на то что в абсолютном большинстве национальных кодексов основным непосредственным объектом выступают общественные отношения в сфере информационной безопасности, ряд законодательств демонстрирует тенденцию к закреплению или фактическому включению факультативных объектов уголовно-правовой охраны.

Как известно, факультативный объект – это социальное благо, которому может быть причинен вред в результате преступления наряду с основным объектом. В контексте преступлений, связанных с вредоносным программным обеспечением, таким объектом могут выступать общественные отношения в сфере собственности, нормального функционирования критической инфраструктуры, экономических интересов, а в отдельных случаях – даже жизни и здоровья граждан, если действия с вредоносным программным обеспечением создают угрозы для этих отношений (например, посредством деструктивного воздействия на программное обеспечение медицинского оборудования, что приводит к его некорректной работе).

Анализируя статьи уголовных кодексов стран Содружества, можно утверждать, что в некоторых из них факультативный объект прямо или косвенно закреплен в диспозициях соответствующих норм. Так, в ч. 2 ст. 273 УК РФ квалифицирующим признаком является причинение крупного ущерба, а в ч. 3 ст. 273 УК РФ – наступление тяжких последствий или создание угрозы их наступления. Эти последствия, как правило, выходят за пределы нарушений в сфере информационной безопасности и затрагивают иные отношения.

Иной подход реализован в уголовном законодательстве Кыргызской Республики. В ст. 320 УК КР в основном составе содержится прямое указание на причинение *значительного ущерба или иного значительного вреда*, что, свидетельствует о защите не только информации, но и иных общественных отношений. Иными словами, можно сделать вывод о том, что такие общественные отношения по кыргызскому уголовному законодательству являются уже не факультативным, а дополнительным объектом преступных действий, связанных с оборотом вредоносных компьютерных программ.

Уголовный кодекс Республики Казахстан предусматривает квалифицированные составы, охватывающие действия в отношении «критически важных объектов информационно-коммуникационной инфраструктуры», что в контексте современной доктрины означает наличие факультативного объекта в виде общественных отношений, связанных с безопасностью жизненно важных

объектов. Подобный подход обоснован тем, что воздействие на такие объекты с помощью вредоносного программного обеспечения может повлечь сбои в сферах энергоснабжения, водообеспечения, транспорта, связи, что, в свою очередь, затрагивает интересы национальной безопасности как таковой.

Аналогичный подход демонстрирует законодатель в ст. 354 УК Республики Беларусь, где указание на использование или сбыт вредоносных программ, предназначенных для нарушения работы компьютерных систем, свидетельствует о стремлении законодателя защитить не только данные, но и технические средства, обеспечивающие функционирование этих данных. В конструкции состава прослеживается факультативный объект – экономическая безопасность

В ст. 379 УК Туркменистана факультативный объект приобретает еще более выраженный характер. Законодатель осознанно охватывает сферу национальной безопасности, так как упоминает об источниках национальной электронной информации, национальной информационной системы и критически важных объектов инфраструктуры.

В ст. 273-1 УК Азербайджана законодатель в предмет преступления включает устройства, коды доступа и иные элементы, которые непосредственно используются в процессе цифрового взаимодействия, имеющие значение для финансово-хозяйственной деятельности, что заслуживает особого внимания. Соответственно, прослеживается в качестве факультативного объекта экономическая составляющая.

В ст. 363 УК Армении прямо указано на наступление по неосторожности тяжких последствий, таких как крупный имущественный ущерб, расстройство деятельности организаций, аварии или уничтожение информации особой ценности. Эта законодательная конструкция прямо вводит в круг факультативных объектов экономическую безопасность (имущественные отношения), нормальное функционирование государственных и коммерческих институтов, общественную безопасность (в случае аварий) и интересы сохранности данных, имеющих критическую важность.

Здесь в целом следует отметить, что в статьях УК Таджикистана, Узбекистана и Молдовы предусматривается повышенная уголовная ответственность за соответствующие действия с вредоносными компьютерными программами, повлекшие тяжкие последствия. Хотя в данных кодексах прямо не указано, что это за последствия, теория и практика позволяют отнести к ним экономический ущерб, дестабилизацию работы крупных предприятий и иных учреждений, нарушение общественного порядка, угрозу для жизни и здоровья многих лиц. Соответственно, эти элементы объективной стороны свидетельствуют о наличии иных охраняемых благ (наряду с информационной безопасностью).

Таким образом, сравнительный анализ позволяет утверждать, что законодательство стран СНГ в различной степени учитывает наличие факультативного непосредственного объекта при описании преступлений, связанных с вредоносными программами. Некоторые страны прямо указывают на ущерб или последствия через квалифицирующие признаки, а другие страны закрепляют это через предмет или способ посягательства. Существующие различия являются подтверждением специфики национальных подходов, а также показателем степени зрелости правовой системы.

Анализ объективной стороны преступлений, связанных с вредоносными программами стран СНГ демонстрирует значительное сходство, но и ярко выраженные особенности.

В ст. 273 УК РФ законодатель ограничился тремя основными действиями – созданием, использованием или распространением вредоносных программ. В то же время в уголовных кодексах Кыргызстана, Казахстана, Таджикистана, Туркменистана и Узбекистана объективная сторона преступления выражена через четыре альтернативных действия, где к указанным трем добавлено еще одно – *внесение изменений в существующие программы*. Такой подход отражает стремление законодателей этих стран более точно охватить все возможные способы создания вредоносного программного обеспечения, особенно актуальные в современных условиях, когда злоумышленники часто не создают вредоносные программы «с нуля», а приспосабливают уже существующее легальное

программное обеспечение, встраивая в него вредоносный функционал. Можно сказать о том, что принципиальных различий здесь нет и такая доработка легального программного обеспечения отвечает всем признакам создания по смыслу той же ст. 273 УК РФ. Согласиться с этим нельзя, поскольку результатом модифицирующих действий злоумышленника не становится появление *новой вредоносной компьютерной программы*, он ее попросту не создает. Внесение изменений приводит лишь к частичной коррекции функционала *существовавшего* программного продукта, который в результате приобретает вредоносный потенциал, но не может считаться вновь созданной программой.

Белорусский законодатель в ст. 354 УК РБ пошел по несколько иному пути, сохранив три основных действия – разработку, использование или распространение, но добавив в качестве четвертого самостоятельного действия *сбыт вредоносных программ*. Это свидетельствует об особом внимании белорусского законодателя к криминализации именно коммерческого оборота вредоносного программного обеспечения, что особенно актуально в условиях развития подпольных рынков киберпреступных услуг (компьютерная атака как услуга), где вредоносные программы активно продаются и покупаются.

Особенность объективной стороны, предусмотренной ст. 273-1 УК Азербайджана является пресечение не только создания, использования, но и всю цепочку оборота: ввоз, продажу, распространение, включая *приобретения для использования.*

В Молдове ст. 260 УК Республики Молдова криминализирует неправомерные производство, импорт, продажу или предоставление технических средств или программных продуктов, разработанных или адаптированных для целей совершения киберпреступлений. Молдавский законодатель, подобно азербайджанскому, уделил особое внимание пресечению оборота средств для киберпреступлений, но при этом ввел ответственность не только для физических, но и для юридических лиц, что является достаточно редким для уголовного законодательства стран Содружества подходом.

Пожалуй, особой спецификой обладает ст. 379 УК Туркменистана, так как имеет сложную совокупность альтернативных действия объективной стороны преступления. Так, объективная сторона ст. 379 УК Туркменистана включается в себя: незаконное уничтожение информации, создание компьютерных программ для нарушения работы систем, производство программной продукции, внесение изменений в существующие программы, их блокировку, изменение формата, копирование, а также преднамеренное использование или распространение таких программ.

Важно подчеркнуть, что туркменский законодатель объединил в одной норме как действия направленные против информация, так и деятельность по созданию и распространению вредоносных компьютерных программ. А также, подобно коллегам из Казахстана, Кыргызстана и других стран СНГ, отдельно выделяет «внесение изменений в имеющиеся программы» как самостоятельное противоправное действие, что подчеркивает актуальность борьбы с модификацией легального программного обеспечения в преступных целях.

По такому же пути пошел и законодатель Республики Армении, однако особенность в конструировании объективной стороны имеется. Она выражается в ещё более детализированном перечне альтернативных действия, который включает в себя: незаконный оборот: производство, изготовление, разработка, импорт, приобретение, хранение, перемещение, поставка, экспорт, а также реализация или использование специальных средств или вирусных программ. Такая детализированная конструкция охватывает всю цепочку – от этапа разработки и ввоза инструментов на территорию страны до их хранения, перемещения и конечной продажи или применения. Наблюдается смещения акцента с самого акта кибератаки на пресечении угрозы на максимально ранней стадии.

Таким образом, анализ уголовного законодательства стран Содружества показывает, что при общей схожести подходов к криминализации создания, использования или распространения вредоносных программ, в каждой стране имеются свои особенности конструирования составов этих преступлений. Если одни страны делают акцент на самих действиях по созданию и модификации

вредоносного программного обеспечения, то другие уделяют больше внимания пресечению их оборота и коммерческого использования. Эти различия отражают как особенности национальных подходов к борьбе с киберпреступностью, так и стремление законодателей учесть специфику современных киберугроз, которые постоянно эволюционируют и требуют адекватного правового реагирования.

В большинстве стран базовые составы преступлений в сфере обращения вредоносного программного обеспечения сконструированы как формальные, т.е. предполагающие окончание преступления в момент совершения деяния – создания, использования или распространения вредоносной программы – независимо от наступления каких-либо последствий. Такой подход зафиксирован, например, в ч. 1 ст. 273 УК РФ, в которой законодатель не связывает наступление уголовной ответственности с причинением вреда, а ограничивается указанием на заведомо вредоносный характер программ и их целевое назначение – уничтожение, блокирование, модификация, копирование информации либо нейтрализация средств защиты.

Аналогичный формальный характер имеет конструкция основного состава преступления в ст. 210 УК Казахстана, 303 УК Таджикистана, 363 УК Армении и 278-6 УК Узбекистана. Во всех этих случаях преступление считается оконченным с момента совершения хотя бы одного из указанных в диспозиции действий, будь то создание, модификация, использование или распространение вредоносной программы. Такой подход обусловлен высокой степенью общественной опасности самого деяния, которое даже без наступления конкретных вредных последствий создает угрозу для безопасности информационной среды.

Материальные конструкции составов, требующие обязательного наступления указанных в законе последствий, представлены в ст. 273-1 УК Азербайджана и в ст. 320 УК Кыргызстана, где ответственность за деяния с вредоносными программами наступает только при условии причинения *значительного ущерба или иного значительного вреда*.

Что касается квалифицирующих признаков, то в законодательстве стран СНГ прослеживается определенное единство в их формулировке. Наиболее

распространенными квалифицирующими обстоятельствами выступают совершение деяния группой лиц по предварительному сговору, организованной группой, с использованием служебного положения, а также из корыстных побуждений. Они свидетельствуют о более высокой степени общественной опасности деяния, что закономерно приводит к ужесточению санкций.

Сравнительно-правовой анализ уголовного законодательства стран Содружества позволяет выявить относительное единство и в определении признаков субъекта и субъективной стороны соответствующих составов преступлений.

Субъектом преступлений, как правило, признается физическое вменяемое лицо, достигшее возраста 16 лет. Однако существуют и особенности. Так, в соответствии с ч. 2 ст. 21 УК Республики Молдова уголовная ответственность, предусмотренная ст. 260 УК Республики Молдова наступает с 14 лет. Кроме того, в УК Молдовы прямо предусмотрена возможность привлечения к уголовной ответственности юридических лиц.

Специальных признаков субъекта (например, наличие определенного статуса, должности, уровня профессиональной подготовки) в основных составах не предусматривается. Однако, многие страны СНГ предусматривают признаки специального субъекта, закрепляя это через квалифицирующий признак, совершение преступления «с использованием служебного положения» (ч. 2 ст. 273 УК РФ, ст. 210 УК РК и др.).

Субъективная сторона анализируемых преступлений характеризуется прямым умыслом. В большинстве случаев диспозиции норм прямо указывают на необходимость осознания виновным назначения программ как вредоносных. Так, в ст. 273 УК РФ говорится о «заведомо предназначенных» для причинения вреда программах, что требует от правоприменителя установления сознательной ориентированности деяния на совершение действий именно с такими программами. Аналогичные выражения – «заведомо предназначенных», «умышленное использование», «с целью» – присутствуют в ст. 320 УК КР, 303 УК Таджикистана, 256 УК Армении, 379 УК Туркменистана.

В отдельных случаях диспозиции указывают на наличие специальной цели – несанкционированный доступ, уничтожение информации, вмешательство в работу информационной системы.

Обобщая, можно сделать вывод, что уголовное законодательство стран СНГ выражает достаточно согласованный подход к характеристике субъекта и субъективной стороны преступлений, связанных с вредоносными программами. Однако имеются и значимые отличия.

Анализ уголовного законодательства стран Содружества позволяет выделить подход, при котором ответственность устанавливается не только за создание, использование или распространение вредоносных программ, но и за такие действия, *как приобретение и (или) хранение* соответствующих программных или аппаратных средств. Наиболее детализированный подход к конструировании объективной стороны выражен в УК Республики Армении, а также прослеживается в УК Азербайджана и Молдовы. Криминализация *приобретения и (или) хранения* позволяет правоприменительным органам вмешиваться на самых ранних этапах преступной деятельности, пресекая подготовку к кибератакам и разрушая инфраструктуру теневого рынка вредоносного инструментария до того момента, как будет причинен реальный ущерб. Это создает правовую основу для противодействия накоплению «цифровых средств совершения преступлений» и повышает эффективность борьбы с организованными формами киберпреступности.

В ходе сравнительно-правового анализа выявлен подход, при котором основной состав преступления сконструирован как материальный, т.е. требующий обязательного наступления указанных в законе последствий. Наиболее отчетливо этот подход прослеживается в ст. 273-1 УК Азербайджана и в ст. 320 УК КР, где ответственность за деяния с вредоносными программами наступает только при условии причинения *значительного ущерба или иного значительного вреда*. Пожалуй, один из минусов проявляется в контексте создания, распространения вредоносных программ, если эти действия не привели к ущербу, что оставляет за

рамками уголовно-правовое воздействие. Положительным критерием можно считать наличие четкого и объективного критерия общественной опасности.

Следует подчеркнуть наличие различных подходов к регулированию оборота идентификаторов доступа. В частности, в УК Азербайджана и УК Республики Молдовы ответственность за действия с паролями, кодами доступа и аналогичными данными интегрирована в нормы об обороте средств для совершения киберпреступлений. На этом фоне выделяется пробельность уголовного законодательства Кыргызской Республики, ответственность за подобные деяния напрямую не предусмотрена. Данное обстоятельство следует расценивать как значимый пробел в правовом регулировании, особенно с учетом того, что в Российской Федерации аналогичные общественно опасные деяния выделены в отдельный состав преступления, предусмотренный ст. 274^5 УК РФ.

Специально основание для освобождения от уголовной ответственности закрепляется в ст. 363 УК Республики Армении, которое имеет следующее содержание. Лицо, добровольно передавшее компетентному органу программное или инструментальное средство или программу, подпадающие под признаки преступления, освобождается от ответственности по этой статье. Данное основание является ярким примером для реализации позитивного посткриминального поведения.

ГЛАВА 2. УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА СОЗДАНИЯ, ИСПОЛЬЗОВАНИЯ И РАСПРОСТРАНЕНИЯ ВРЕДОНОСНЫХ КОМПЬЮТЕРНЫХ ПРОГРАММ ПО ЗАКОНОДАТЕЛЬСТВУ РОССИЙСКОЙ ФЕДЕРАЦИИ И КЫРГЫЗСКОЙ РЕСПУБЛИКИ

§ 1. Объект создания, использования и распространения вредоносных компьютерных программ (ст. 273 УК РФ, ст. 320 УК КР)

Кардинальная трансформация структуры общественных отношений, обусловленная стремительным развитием цифровых технологий, выдвинула на первый план проблему обеспечения информационной безопасности. В этом контексте действия с вредоносными программами перестало быть сугубо технической проблемой, превратившись в сложный правовой вызов, требующий адекватного и четкого законодательного реагирования.

С момента установления уголовной ответственности за действия с вредоносными компьютерными программами прошло почти 30 лет, но научная полемика не утихает до настоящего времени. Без преувеличения можно отметить, что одним из самых дискуссионных вопросов в доктрине уголовного права остается содержание объекта таких преступных посягательств.

Причиной отсутствия некоего теоретического консенсуса в отношении характеристики объекта, пожалуй, является сама имманентная специфика компьютерных преступлений. В целом она заключается в том, что совершаемые деяния посягают не только на общественные отношения в сфере компьютерной информации, но и на другие правоохраняемые блага[91].

Эволюция научных взглядов на объект и предмет преступления, предусмотренного ст. 273 УК РФ, думается, представляет собой переход от сугубо

[91] См.: Корпеев А.Г. Об объекте преступлений, совершаемых с использованием информационно-телекоммуникационных сетей, по уголовному законодательству России и Туркменистана // Юридический аналитический журнал. 2022. Т. 17. № 1. С. 30.

технического и весьма узкого понимания к системному, функциональному и правозащитному подходу. Эти изменения во многом обусловлены развитием цифровых технологий, ростом угроз в сфере информационной безопасности и потребностью механизма уголовно-правовой охраны реагировать на вызовы цифровой эпохи. Законодателем вносилось множество изменений в УК КР, но, к сожалению, сама ст. 320 УК КР не стала предметом активной научной дискуссии и не претерпела значительной эволюции в доктринальном толковании.

Как справедливо отметил К.Н. Евдокимов, наименьшие сложности в доктрине вызывает определение родового объекта ст. 273 УК РФ, что обусловлено ее расположением в гл. 28 раздела «Преступления против общественной безопасности и общественного порядка»[92]. Аналогичным образом обстоит дело и с определением родового объекта ст. 320 УК КР: несмотря на значительные изменения, вносимые в УК КР, ст. 320 УК КР (гл. 40) сохранила свою принадлежность к одноименному разделу, как и в УК КР 1997 г.[93]

Таким образом, родовым объектом как ст. 273 УК РФ, так и ст. 320 УК КР являются общественные отношения в сфере обеспечения общественной безопасности и общественного порядка.

В российской доктрине уголовного права определение видового объекта исследуемого преступления является дискуссионным. В научной литературе по этому поводу сформировался ряд подходов.

Одни авторы (М.М. Малыковцев[94], Д.М. Молчанов[95] и др.) формулируют его узко, фокусируясь на безопасности информации и нормальном порядке функционирования компьютерных систем и ресурсов.

---

[92] См.: Евдокимов К.Н. К вопросу об объекте преступления при создании, использовании и распространении вредоносных программ для ЭВМ (ст. 273 УК РФ) // Сибирский юридический вестник. 2009. № 4. С. 39.

[93] Уголовный кодекс Кыргызской Республики от 1 октября 1997 г. № 68 (утратил силу с 1 января 2019 г. в соответствии с Законом Кыргызской Республики от 24 января 2017 г. № 10) [Электронный ресурс]. URL: https://cbd.minjust.gov.kg/3-10/edition/919984/ru (дата обращения: 19.08.2025).

[94] См.: Малыковцев М.М. Уголовная ответственность за создание, использование и распространение вредоносных программ для ЭВМ: дис. ... канд. юрид. наук. М., 2006. С. 62.

[95] См.: Бимбинов А.А., Боженок С.А., Грачева Ю.В. и др. Уголовное право Российской Федерации. Особенная часть: учебник / под ред. И. Э. Звечаровского. М., 2020. С. 454.

Другие исследователи предлагают более широкие трактовки. Например, К.А. Барышева включает в него всю совокупность общественных отношений в информационной сфере[96], а Е.В. Лошенкова[97] детализирует его через обеспечение конфиденциальности, целостности, доступности информации и безопасности операций с ней. Наиболее комплексный подход, интегрирующий объект в систему защиты национальных интересов, предлагает Д.В. Пучков[98], определяя его через состояние защищенности личности, общества и государства от информационных угроз.

В научной доктрине Кыргызской Республики, судя по представленным точкам зрения, также присутствует дискуссия, однако с иным акцентом. З.К. Курманов и Р.А. Оконова непосредственно определяют групповой (видовой) объект компьютерных преступлений как информационную безопасность, но сразу же уточняют, что она является видом общественной безопасности, тем самым изначально встраивая его в более широкий контекст охраняемых благ[99]. В свою очередь, И.Л. Голобородько[100] определяет видовой объект как общественные отношения, непосредственно связанные с информационной сферой, без дальнейшей детализации.

Следует отметить, что в Российской Федерации основополагающим документом, регламентирующим вопросы информационной безопасности, выступает Доктрина информационной безопасности РФ, утвержденная Указом Президента РФ от 5 декабря 2016 г. № 646 (далее – Доктрина)[101].

---

[96] См.: Барышева К.А., Грачева Ю.В., Долотов Р.О. и др. Российское уголовное право. Особенная часть: учебник / под ред. Г. А. Есакова. М., 2021. С. 450–451.

[97] Уголовное право. Особенная часть: учебник для бакалавров / под ред. А.И. Чучаева. 3-е изд., перераб. и доп. М., 2018. С. 403.

[98] См.: Пучков Д.В. Уголовно-правовая модель защиты телекоммуникаций от преступных посягательств: проблемы теории и практики: дис. ... д-ра юрид. наук. Екатеринбург, 2022. С. 6.

[99] См.: Курманов К.Ш. Уголовное право Кыргызской Республики (Особенная часть): учебник / под ред и с предисл. К. Ш. Курманова. Бишкек, 2001. С. 387.

[100] См.: Голобородько И.Л. Преступления в компьютерной сфере // Научные исследования в Кыргызской Республике. 2025. № 2. С. 110.

[101] Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации [Электронный ресурс]. URL: https://www.garant.ru/products/ipo/prime/doc/71456224/ (дата обращения: 19.08.2025).

Аналогичным образом в Кыргызской Республике вопросы обеспечения безопасности в информационной сфере регулируются Законом КР от 17 июля 2024 г. «О кибербезопасности Кыргызской Республики»[102], который определяет правовые основы формирования единой государственной системы кибербезопасности. Кроме того, концептуальные основы защиты национальных интересов в информационной сфере закреплены в Концепции национальной безопасности Кыргызской Республики, утвержденной Указом Президента КР от 20 декабря 2021 г. № 570 (далее – Концепция)[103]. Этот документ раскрывает содержание понятия информационной безопасности как неотъемлемой составляющей национальной безопасности, определяет потенциальные угрозы и стратегические приоритеты государства в данной области.

Согласно Доктрине и Концепции под информационной безопасностью следует понимать состояние защищенности личности, общества и государства от информационных угроз. Исходя из вышеизложенного и с учетом современных реалий цифровой трансформации, по нашему мнению, видовой объект создания, использования и распространения вредоносных компьютерных программ можно определить как *общественные отношения, обеспечивающие цифровую безопасность как неотъемлемый элемент общественной безопасности, гарантирующие защищенность жизненно важных интересов личности, общества и государства посредством обеспечения конфиденциальности, целостности, доступности и аутентичности компьютерной информации, а также устойчивого и безопасного функционирования информационно-телекоммуникационной инфраструктуры как критически важного компонента современного цифрового общества.*

Переходя к анализу непосредственного объекта ст. 273 УК РФ и ст. 320 УК КР, следует подчеркнуть его принципиальную взаимосвязь с видовым объектом,

---

[102] Закон Кыргызской Республики от 17 июля 2024 г. № 121 «О кибербезопасности Кыргызской Республики» [Электронный ресурс]. URL: https://cbd.minjust.gov.kg/4-5371/edition/13381/ru (дата обращения: 19.08.2025).

[103] Указ Президента Кыргызской Республики от 20 декабря 2021 г. УП № 570 «О Концепции национальной безопасности Кыргызской Республики» [Электронный ресурс]. URL: https://cbd.minjust.gov.kg/5-9804/edition/1118040/ru (дата обращения: 19.08.2025).

рассмотренным ранее. В российской доктрине уголовного права отсутствует единая позиция относительно определения непосредственного объекта ст. 273 УК РФ, что отражает сложность и многогранность самого явления.

Е.В. Лошенкова определяет непосредственный объект исследуемого преступления как общественные отношения, складывающиеся по поводу обеспечения целостности и доступности компьютерной информации[104], акцентируя внимание на защите ключевых свойств информации.

И.А. Ефремова предлагает более узкий подход к определению непосредственного объекта, а именно информационную безопасность конкретной компьютерной безопасности[105].

В контексте многообъектности состава преступления, предусмотренного ст. 273 УК РФ, следует обратиться к мнению К. Н. Евдокимова, который полагает, что основной состав (ч. 1 ст. 273 УК РФ) имеет формальный состав и посягает на основной непосредственный объект. При этом прямой ущерб имуществу, правам личности или государства не является обязательным. Поэтому другие охраняемые блага (жизнь, здоровье, конституционные права, интересы службы и т.д.) выступают здесь лишь в качестве факультативного объекта. А в качестве дополнительного непосредственного объекта ч. 2, 3 ст. 273 УК РФ выделяет общественные отношения, обеспечивающие законные права и интересы лиц в сфере собственности или интересы службы (государственной, муниципальной, коммерческий и т.д.), где вред этим благам является обязательным признаком преступления[106].

Е.Л. Харьковский включает в основной непосредственный объект преступления техническую безопасность систем, весь комплекс публичных интересов, прав обладателей информации и операторов систем, связанных с законным оборотом компьютерной информации и безопасным

---

[104] См.: Уголовное право. Особенная часть: учебник для бакалавров / под ред. А. И. Чучаева. 3-е изд., перераб. и доп. С. 403.

[105] См.: Ефремова И.А. Уголовное право (Особенная часть): курс лекций / под ред. и с предисл. Б. Т. Разгильдиева; Саратовская государственная юридическая академия. Саратов, 2023. С. 336.

[106] См.: Евдокимов К.Н. Противодействие компьютерной преступности: теория, законодательство, практика: дис. ... д-ра юрид. наук. М., 2021. С. 309.

функционированием всей информационно-телекоммуникационной инфраструктуры[107].

В кыргызской доктрине наблюдается ограниченное количество мнений относительно непосредственного объекта преступления, предусмотренного ст. 320 УК КР, по сравнению с российской доктриной, что, пожалуй, свидетельствует о меньшей степени разработанности проблемы.

На раннем этапе осмысления компьютерных преступлений, З.К. Курмановым и Р.А. Океновой была сформулирована позиция относительно непосредственного объекта преступления как права владельца компьютерной системы на неприкосновенность информации (программного обеспечения)[108]. В настоящее время, И.Л. Голобородько дает определение непосредственного объекта через целостность, доступность либо конфиденциальность компьютерной информации[109].

При определении основного непосредственного объекта ст. 273 УК РФ и ст. 320 УК КР стоит согласиться с позицией Е.А. Русскевича, рассматривающего под непосредственным объектом ст. 273 УК РФ общественные отношения, связанные с обеспечением информационной безопасности от деструктивного воздействия вредоносной компьютерной информации и вредоносных компьютерных программ[110].

При этом факультативный непосредственный объект, который может быть нарушен в зависимости от конкретных обстоятельств совершения деяния, охватывает широкий спектр охраняемых уголовным законом благ, таких как интересы службы, конституционные права и свободы человека, общественная безопасность и иные ценности, которым может быть причинен вред в результате противоправного деяния, предусмотренного ст. 273 УК РФ и ст. 320 УК КР.

---

[107] См.: Дворянксков И.В. Уголовное право. Особенная часть: учебник / под ред. д-ра юрид. наук, проф. И. В. Дворянскова. М.: ИНФРА-М, 2025. С. 387–388.
[108] См.: Курманов К.Ш. Указ. соч. С. 387.
[109] См.: Голобородько И.Л. Указ. соч. С. 111.
[110] См.: Калиниченко И.А., Андреев А.В., Галиев Д.В. и др. Противодействие преступлениям в сфере информационных технологий: учебник / под науч. ред. И. А. Калиниченко; под техн. ред. В. В. Гончара. М., 2025. С. 137.

Наибольший интерес, теоретическую сложность и несомненную практическую значимость представляет вопрос об определении предмета исследуемого преступления.

Как верно и в то же время афористично отмечает Л.В. Иногамова-Хегай, «предмет преступления есть объект объекта преступления»[111], что подчеркивает его роль как неотъемлемого элемента структуры преступного деяния в тех составах, где его наличие прямо предусмотрено законодателем.

В отечественной доктрине вокруг предмета ст. 273 УК РФ ведутся оживленные дискуссии. Ряд авторов (И.А. Ефремова[112], В.С. Изосимов[113]) придерживаются узкой трактовки, определяя в качестве предмета исключительно вредоносную программу для ЭВМ.

В противовес этому А.Г. Кибальник в качестве предмета преступления выделяет только компьютерную информацию[114]. Другие исследователи предлагают более широкую трактовку: так, по мнению Т.И. Ваулиной, предметом рассматриваемого преступления является вредоносная компьютерная программа или иная компьютерная информация[115].

С.М. Корабельников считает, что предметом преступления является информация, а также компьютерные программы[116]. А.С. Червоткин в качестве предмета преступления определяет компьютерную информацию или средства защиты компьютерной информации[117]. Важно отметить, что разногласия среди

---

[111] Иногамова-Хегай Л.В. Уголовное право Российской Федерации. Общая часть: учебник / под ред. д-ра юрид. наук, проф. Л.В. Иногамовой-Хегай. 3-е изд., перераб. и доп. М., 2022. С. 60.

[112] См.: Ефремова И.А. Уголовное право (Особенная часть): курс лекций / под ред. и с предисл. Б. Т. Разгильдиева. С. 336.

[113] См.: Бастрыкин А.И., Чучаев А. И. Уголовное право. Особенная часть: учебник для вузов / под общ. ред. А.И. Бастрыкина ; под науч. ред. А. И. Чучаева. М., 2025. С. 328.

[114] См.: Наумов А.В., Кибальник А. Г. Преступления против общественной безопасности и общественного порядка: учебник для вузов / отв. ред. А.В. Наумов, А. Г. Кибальник. 6-е изд., перераб. и доп. М., 2025. С. 153.

[115] См.: Козаченко И.Я., Новоселов Г.П. Уголовное право. Особенная часть: учебник / отв. ред. И. Я. Козаченко, Г. П. Новоселов. 5-е изд., изм. и доп. М., 2013. С. 708.

[116] См.: Корабельников С.М. Преступления в сфере информационной безопасности: учеб. пособие для вузов. М., 2024. С. 78.

[117] См.: Лебедев В.М. Комментарий к Уголовному кодексу РФ: в 4 т. / отв. ред. В. М. Лебедев. М., 2025. Т. 3. Особенная часть. Раздел IX. С. 290.

авторов существуют как по вопросу о том, что входит в предмет преступления (его объем), так и по вопросу о том, должен ли этот предмет обязательно обладать свойством «вредоносности».

Законодатель Кыргызской Республики в ст. 320 УК КР подошел к формулировке иначе. Несмотря на то что ст. 320 УК КР называется «Создание вредоносных программных продуктов», непосредственно в самой диспозиции нормы используется термин «программный продукт», что потенциально позволяет расширить предмет рассматриваемого преступления по сравнению со ст. 273 УК РФ.

Думается, что кыргызский подход, как показано в § 3 гл. 1, ближе к «технологически нейтральным» моделям отдельных стран СНГ (например, Армении и Туркменистана), где акцент делается на функциональной предназначенности объекта, а не на его формальном наименовании.

Определение компьютерной программы содержится в Законе КР от 14 января 1998 г. № 6 «Об авторском праве и смежных правах», где согласно п. 29 ст. 4 программой для ЭВМ является совокупность инструкций или правил, выраженных словами, цифрами, кодами, символами, знаками или в какой-либо другой форме, предназначенных для функционирования ЭВМ и других компьютерных устройств для достижения определенной цели или результата[118].

Ключевым признаком здесь является функциональное назначение объекта как программы, т.е. его способность быть исполненным компьютером для автоматического совершения заданных действий. Употребление законодателем термина «программный продукт» вместо более узкого «программа для ЭВМ» не расширяет предмет преступления на любые виды компьютерной информации или данные, а, напротив, подчеркивает его завершенность и свойство быть продуктом, готовым к использованию в качестве инструмента киберпреступления. Это толкование напрямую вытекает из принципа юридической определенности (ст. 3

[118] Закон Кыргызской Республики от 14 января 1998 г. № 6 «Об авторском праве и смежных правах» [Электронный ресурс]. URL: https://cbd.minjust.gov.kg/17/edition/1240396/ru (дата обращения: 21.08.2025).

УК КР), требующего формальной четкости уголовного закона, и подтверждается системным соотношением со ст. 319 УК КР, где законодатель отдельно оперирует понятием «компьютерная информация», тем самым разводя эти два разных предмета преступного посягательства.

Таким образом, правоприменитель не только может, но и обязан руководствоваться определением из авторского права, поскольку это единственное легальное определение, обеспечивающее единообразие понимания термина во всей национальной правовой системе Кыргызстана и предотвращающее произвольное расширительное толкование уголовно-правовой нормы.

Однако же остается нерешенным вопрос о том, должен ли этот предмет обладать свойством «вредоносности»? Думается, что предмет преступления по ст. 273 УК РФ и ст. 320 УК КР в обязательном порядке должен обладать свойством «вредоносности».

Важно отметить, что законодательная техника описания вредоносных свойств программы в ст. 273 УК РФ и ст. 320 УК КР различается, что отражает разные подходы к пониманию самой сути «вредоносности».

Так, диспозиция ст. 273 УК РФ, по сути, определяет вредоносность через заложенный в программу потенциал: она должна быть *заведомо предназначена для несанкционированного уничтожения, блокирования, модификации, копирования информации или нейтрализации средств защиты*.

В свою очередь, кыргызский законодатель пошел по пути более широкого подхода. Перечень в ст. 320 УК КР является более расширенным. Помимо несанкционированного уничтожения, копирования, блокирования, изменения информации и нейтрализации средств защиты, которые присутствуют и в ст. 273 УК РФ, кыргызский законодатель дополнительно указывает на *несанкционированный доступ и копирование, нарушение работы информационных систем или сети электросвязи*.

Указание на «несанкционированный доступ и копирование» в ст. 320 УК КР означает, что под действие этой статьи подпадают и так называемые инструменты несанкционированного доступа (например, бэкдоры, эксплойты, сканеры

уязвимостей), если они заведомо предназначены для проникновения в защищенную информационную систему. Более того, связка «доступ и копирование» предполагает, что предметом преступления могут признаваться и программы, назначением которых является не просто проникновение, но и хищение информации. Это делает диспозицию кыргызской нормы значительно более емкой и соответствующей современным киберугрозам, где часто именно несанкционированный доступ является ключевой стадией для последующих преступных действий.

Ранее, до внесения изменений в 2011 г., ст. 273 УК РФ в качестве уголовно наказуемого последствия закрепляла «нарушение работы ЭВМ, системы ЭВМ или их сети». Стоит отметить, что УК КР 1997 г. также оперировал схожей формулировкой, предусматривая аналогичное последствие. Однако с принятием нового УК КР в 2017 г. законодатель внес существенные корректировки в эту дефиницию, заменив устаревшее понятие «нарушение работы ЭВМ, системы ЭВМ или их сети» на более современное – «нарушение работы системы компьютера или компьютерной сети, или сети электросвязи». Дальнейшее развитие уголовного законодательства привело к еще одному обновлению данной нормы, и в настоящее время действующая редакция УК КР оперирует конструкцией в виде «нарушения работы информационных систем или сети электросвязи», что отражает эволюцию терминологии и расширение охвата защищаемых объектов в цифровую эпоху.

Содержательная сторона признака в виде «нарушения работы информационных систем или сети электросвязи», используемого в ст. 320 УК КР, раскрывается через отсылочные нормы к отраслевому законодательству. Так, понятие «информационная система» определено в п. 3 ст. 2 Закона КР от 19 июля 2017 г. № 127 «Об электронном управлении»[119], где оно трактуется как совокупность информации, содержащейся в базах данных, и обеспечивающих ее обработку информационных технологий и технических средств. В свою очередь,

[119] Закон Кыргызской Республики от 19 июля 2017 г. № 127 «Об электронном управлении» // Газета «Эркин-Тоо». 2017. 25 июля. № 127. URL:https://cbd.minjust.gov.kg/111634/edition/36815/ru (дата обращения: 15.02.2026).

дефиниция «сети электросвязи» закреплена в Законе КР «Об электрической связи»[120], под которой понимается проводная, радио-, оптическая или иная электромагнитная система, предназначенная для направления, коммутации или передачи сообщений электросвязи, включая голосовые, звуковые, визуальные сообщения, данные и изображения.

Однако необходимо отметить, что оба этих закона – и «Об электронном управлении», и «Об электрической связи» – в соответствии с Законом КР от 31 июля 2025 г. № 179[121] утрачивают свою силу в связи с введением в действие Цифрового кодекса КР. Складывается ситуация, при которой понятия «информационная система» и «сеть электросвязи» являющиеся ключевыми элементами состава преступления теряют свои действующие легальные определения. Следовательно, в ближайшее время, с большой долей вероятности прогнозируется, что законодателем Кыргызской Республики будут инициированы очередные изменения в уголовном законе, которые будут направлены на приведение в соответствие ст. 320 УК КР с новой терминологической базой Цифрового кодекса КР.

«Вредоносность» - это юридическая характеристика, а не техническая функция, если рассуждать с точки зрения уголовного права, она определяется предназначением и даже в какой-то степени умыслом виновного. Ведь, уголовный закон оперирует деяниями человека, наделенного сознанием, а не безликими алгоритмами. По сути, свойство «вредоносности» программы приобретается не в силу своего кода, а в силу замысла лица, которые ее создает или использует. Так, правовая сущность «вредоносности» заключатся изначальной предназначенности программы в целях осуществления противоправной деятельности.

Анализ изменений уголовного законодательства России и Кыргызской Республики в сфере киберпреступности позволяет выявить не только динамику

---

[120] Закон Кыргызской Республики от 2 апреля 1998 г. № 31 «Об электрической связи» // Газета Ведомости Жогорку Кенеша Кыргызской Республики. 1998. № 8. Ст. 230а. URL: https://cbd.minjust.gov.kg/4-31/edition/36653/ru?lang=ru (дата обращения: 15.02.2026).

[121] Закон Кыргызской Республики от 31 июля 2025 г. № 179 «О введении в действие Цифрового кодекса Кыргызской Республики» // Газета «Эркин-Тоо». 2025. 5 авг. № 195. URL: https://cbd.minjust.gov.kg/4-5604/edition/35394/ru (дата обращения: 20.02.2026)

развития правовых норм, но и актуальные проблемы, например, связанные с понятийно-категориальным аппаратом.

В настоящее время одной из ключевых проблем уголовной политики в сфере противодействия киберпреступности выступает необходимость унификации понятийно-категориального аппарата, что обусловлено спецификой компьютерных преступлений, их динамичным развитием и трансграничным характером. В научной литературе активно исследуются такие основополагающие понятия, как «киберпреступность»[122], «киберпространство»[123], «цифровая информация»[124], «виртуальная среда»[125] и др., однако их содержание зачастую трактуется неоднозначно, что создает сложности как для законодательного регулирования, так и для правоприменительной практики. По понятным причинам в рамках данного исследования особый интерес представляет анализ понятия «вредоносная программа» и ее нормативно-правовое закрепление.

В Соглашении о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий, ратифицированном как Российской Федерацией, так и Кыргызской Республикой[126], дается определение вредоносной программы, под которой понимается созданная или существующая программа со специально внесенными изменениями, заведомо приводящая к несанкционированному уничтожению,

---

[122] См.: Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дис. ... канд. юрид. наук. Владивосток, 2005. С. 39.
[123] См.: Лихачев Н.А. Указ. соч. С. 94.
[124] См.: Бегишев И.Р. Понятие и виды преступлений в сфере обращения цифровой информации: дис. ... канд. юрид. наук. Казань, 2017. С. 34.
[125] См.: Дремлюга Р.И., Крипакова А.В. Преступления в виртуальной реальности: миф или реальность? // Актуальные проблемы российского права. 2019 № 3. С. 161–169.
[126] Закон Кыргызской Республики от 21 января 2020 г. № 14 «О ратификации Соглашения о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий, подписанного 28 сентября 2018 года в городе Душанбе» // Газета «Эркин Тоо». 2020. 24 янв. № 7 (3079). URL: https://cbd.minjust.gov.kg/4-2809/edition/992067/ru (дата обращения: 13.02.2025).

блокированию, модификации либо копированию информации, нарушению работы информационной (компьютерной) системы[127].

В Российской Федерации определение вредоносной программы закреплено в п. 2.6.5 и 2.6.6 ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»[128], в п. 4 постановления Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37, с учетом ст. 1261 ГК РФ[129].

В научной среде понятие «вредоносной программы» исследуется такими учеными как М.М. Малыковцев[130], В.Б. Вехов[131], К.Н. Евдокимов[132], Е.А. Маслакова[133], И.Р. Бегишев[134] и др.

По мнению Е.А. Русскевича, традиционное определение вредоносности программы, основанное на ее способности вызывать несанкционированное уничтожение, блокирование, модификацию или копирование информации, не охватывает весь спектр современных угроз[135]. Действительно, с каждым годом вредоносные программы обретают более серьезную форму угрозы в связи с развитием информационных технологий.

---

[127] Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий 2018 г. // Законодательство стран СНГ. URL: https://base.spinform.ru/show_doc.fwx?rgn=110821 (дата обращения: 13.02.2025).

[128] ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. М., 2008.

[129] 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». URL: https://www.consultant.ru/document/cons_doc_LAW_434573/ (дата обращения: 15.02.2025).

[130] См.: Малыковцев М. М. Указ. соч. С. 10.

[131] См.: Вехов В. Б. Вредоносные компьютерные программы как предмет и средство совершения преступления // Расследование преступлений: проблемы и пути их решения. 2015. № 2 (8). С. 45.

[132] См.: Евдокимов К. Н. Создание, использование и распространение вредоносных компьютерных программ: уголовно-правовые и криминологические аспекты: монография. Иркутск, 2013. С. 60.

[133] См.: Маслакова Е. А. Незаконный оборот вредоносных компьютерных программ: уголовно-правовые и криминологические аспекты: дис. ...канд. юрид. наук. Орел, 2008. С. 68.

[134] См.: Бегишев И. Р. Указ. соч. С. 69.

[135] См.: Русскевич Е. А. Понятие вредоносной компьютерной программы // Актуальные проблемы российского права. 2018. № 11. С. 207–215.

В ст. 320 УК КР вместо «вредоносных программ» употребляется термин «программный продукт», но в уголовно-правовом контексте какое-либо разъяснение или закрепление данного понятия отсутствует.

Ранее в нормативно-правовой системе Кыргызской Республики определение программного продукта, точнее, программы для электронных вычислительных машин (далее – ЭВМ), содержалось в Законе Кыргызской Республики от 30 марта 1998 г. № 28 «О правовой охране программ для электронных вычислительных машин и баз данных»[136]. В соответствии с указанным Законом программа для ЭВМ представляла собой объективную форму представления совокупности данных и команд, предназначенных для функционирования ЭВМ и получения определенного результата. В последующем данный закон утратил силу[137]. Однако терминологическая база, содержащаяся в Законе Кыргызской Республики от 30 марта 1998 г. № 28 «О правовой охране программ для электронных вычислительных машин и баз данных» была отражена в Законе Кыргызской Республики от 14 января 1998 г. № 6 «Об авторском праве и смежных правах»[138].

Статья 320 УК КР без нормативного определения криминообразующего признака «программный продукт», конечно же, страдает правовой неопределенностью. Отсутствие легальной дефиниции не позволит не только выработать устойчивую практику по квалификации соответствующих деяний, но и с высокой вероятностью может приводить к злоупотреблениям.

Здесь напрашивается еще один проблемный вопрос: насколько актуальным является использование терминов «вредоносная компьютерная программа» или «компьютерная информация»?

---

[136] Закон Кыргызской Республики от 3 марта 1998 г. № 28 «О правовой охране программ для электронных вычислительных машин и баз данных» // Газета «Эркин-Тоо». 1998. 4 апр. № 28. URL: https://cbd.minjust.gov.kg/39/edition/1240316/ru (дата обращения: 18.02.2025).

[137] Закон Кыргызской Республики от 17 марта 2023 г. № 62 «О внесении изменений в Закон Кыргызской Республики “Об авторском праве и смежных правах” и признании утратившими силу некоторых законодательных актов Кыргызской Республики» // Газета «Эркин-Тоо». 2023. 24 марта. № 62. URL: https://cbd.minjust.gov.kg/112543/edition/1240272/ru (дата обращения: 18.02.2025).

[138] Закон Кыргызской Республики от 14 января 1998 г. № 6 «Об авторском праве и смежных правах» // Газета «Эркин-Тоо». 28.01.1998. № 6. URL: https://cbd.minjust.gov.kg/17/edition/1240396/ru (дата обращения: 18.02.2025).

И.Р. Бегишев, анализируя понятие «цифровая информация», выделяет ее ключевые отличительные признаки и специфику, обосновывая тем самым целесообразность использования именно этого термина вместо традиционного «компьютерная информация»[139].

По мнению И.Р. Бегишева, цифровая информация характеризуется следующим: во-первых, она проста в обработке в информационно-телекоммуникационных устройствах независимо от их назначения (персональный компьютер, сервер, мобильный телефон, планшет, цифровая видеокамера и т.д.); во-вторых, легко передается и обращается в таких устройствах, их системах и сетях; в-третьих, легко создаваема и уничтожаема; в-четвертых, может постоянно находиться лишь в информационно-телекоммуникационном устройстве или временно – в каналах и сетях передачи информации; в-пятых, модифицируется и копируется без особых трудностей. И.Р. Бегишев особо отмечает, что ограничительное понимание компьютерной информации только как информации, находящейся на машинном носителе, в ЭВМ, системе или сети ЭВМ (следуя диспозиции ст. 272 УК РФ в прежней редакции), является неверным, поскольку такая информация может находиться и в других устройствах, например в мобильном телефоне[140].

В современных условиях вредоносные компьютерные программы создаются, используются и распространяются с помощью «иных цифровых устройств», а не только компьютеров, в связи с этим обуславливается необходимость перехода к более широкому понятию «цифровая информация».

Следует подчеркнуть, что действующее законодательство, включая ст. 272 и 273 УК РФ, а также разъяснения постановления Пленума Верховного Суда РФ от

---

[139] Бегишев И. Р. Указ. соч. С. 69.
[140] См.: Бегишев И.Р. Указ. соч. С. 33–34.

15 декабря 2022 г. № 37[141] и Методические рекомендации Генпрокуратуры[142], по-прежнему оставляет в рамках устаревшего подхода и связывает понятие «вредоносной программы» с программами для ЭВМ. Однако, в настоящее время складывается иная картина. Ведь, вредоносная активность давно вышла за пределы классического компьютера и охватывает более широкий спектр устройств: от смартфонов и планшетов до интернет вещей, облачных серверов и даже автомобилей с цифровым управлением. Пожалуй, все это создает правовой вакуум, а также сложности при квалификации действий злоумышленников. Например, вредоносный код, который предназначен для взлома системы «умного дома» или банкомата, формально может не подпадать под узкое определение компьютерной программы.

Особую остроту эта проблема приобретает в Кыргызской Республике, где предприняты шаги по систематизации цифрового законодательства. Так, в п. 89 ч. 1 ст. 1 Цифрового кодекса КР дается определение цифрового устройства как технического устройства, предназначенного для обработки цифровых данных, включая, но не ограничиваясь, электронной вычислительной машиной (ЭВМ)[143].

В этой связи логичным и необходимым шагом видится введение в научный и практический оборот универсального и технологически нейтрального понятия «цифровая вредоносная программа».

Под цифровой вредоносной программой следует понимать *представленную в объективной форме совокупность цифровых данных и команд, предназначенных для несанкционированного функционирования любого цифрового устройства, их*

---

[141] 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». URL: https://www.consultant.ru/document/cons_doc_LAW_434573/ . (дата обращения: 15.02.2026).

[142] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации. М.: Генеральная Прокуратура РФ, 2013. URL: https://epp.genproc.gov.ru/web/gprf/documents (дата обращения: 20.11.2025).

[143] Кодекс КР от 31 июля 2025 г. № 178 «Цифровой Кодекс Кыргызской Республики». URL: https://cbd.minjust.gov.kg/3-48/edition/35412/ru?lang=ru (дата обращения: 25.02.2025).

систем или сетей, следствием чего является уничтожение, блокирование, модификация или копирование цифровой информации, нарушение работы устройства или сети.

Такое определение охватывает весь спектр современных угроз – от классических компьютерных вирусов и троянов до вредоносных скриптов для веб-браузеров, мобильных эксплоитов, программы-вымогатели в среде IoT-устройств и зловредного кода в микроконтроллерах. Унификация терминологии на основе понятия «цифровая информация» и производных от него («цифровое устройство», «цифровая программа») позволит создать последовательную устойчивую правовую базу, обеспечивающую адекватную защиту всей цифровой экосистемы независимо от конкретной аппаратной платформы, на которую нацелена атака.

Данное изменение побуждено объективной реальностью, при которой вредоносное воздействие в современном мире направлено уже не только на ЭВМ, а на всю сложную и взаимосвязанную цифровую среду. Эта среда включает в себя IoT-устройства, киберфизические системы, облачные платформы, распределенные реестры и другие элементы, где программный код выступает универсальным цифровым инструментом, чье функционирование и вредоносный потенциал не зависят от конкретного типа устройства-носителя.

Применительно к законодательству Кыргызской Республики аналогичное предложение по расширению предмета ст. 320 УК КР является не только логичным, но и особенно важным. Существующее противоречие между узким определением программы для ЭВМ в Законе КР от 14 января 1998 г. № 6 «Об авторском праве и смежных правах»[144] и прогрессивным, широким подходом ЦК КР создает правовую неопределенность и ограничивает эффективность борьбы с киберпреступностью. Действительно, ст. 320 УК КР опирается на устаревшую систему взглядов, привязывая преступление к «программам для ЭВМ». Это определение, закрепленное в Законе КР от от 14 января 1998 г. №6 «Об авторском

[144] Закон Кыргызской Республики от 14 января 1998 г. № 6 «Об авторском праве и смежных правах» [Электронный ресурс] // URL: https://cbd.minjust.gov.kg/17/edition/1240396/ru (дата обращения 21.08.2025).

праве и смежных правах» фокусируется на традиционных ЭВМ и не учитывает современную цифровую экосистему.

При этом Цифровой кодекс КР, который является основополагающим актом в цифровой среде демонстрирует иную картину. Как отмечено, п. 87 ч. 1 ст. 1 ЦК КР «цифровое приложение» как цифровой ресурс, то есть программу для ЭВМ и иных цифровых устройств[145].

Таким образом, предложенный термин *«цифровая вредоносная программа»* становится ключевым шагом для адекватного правового реагирования. С его помощью появляется возможность корректно квалифицировать такие действия, как взлом автомобиля с цифровым управлением, атака на системы «умного дома», саботаж промышленных контроллеров или распространение вредоносного кода в сетях IoT, даже если целевое устройство формально не подпадает под устаревшее бытовое или узкотехническое понимание компьютера. Это унифицирует правовые подходы, устранит существующие пробелы и создаст надежную основу для защиты всей цифровой экосистемы по мере ее усложнения.

Не менее актуальным вопросом, в доктрине уголовно права, является содержание предмета преступлений, предусмотренных ст. 273 УК РФ и ст. 320УК КР, а именно, категория «иной вредоносной компьютерной информации».

Для понимания сущности «иной» компьютерной информации в контексте ст. 273 УК РФ необходимо обратиться к законодательному определению базового понятия. Согласно ст. 2 Федерального закона № 149 «Об информации, информационных технологиях и о защите информации»[146] и примечанию 1 к ст. 272 УК РФ, под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. Это родовое понятие, охватывающее любые данные в электронной форме.

---

[145] Кодекс Кыргызской Республики от 31 июля 2025 года № 178 «Цифровой Кодекс Кыргызской Республики». URL: https://cbd.minjust.gov.kg/3-48/edition/35412/ru?lang=ru (дата обращения: 21.08.2025).

[146] Федеральный закон от 26 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 2006. № 31 (ч. 1). Ст. 3448.

Однако предмет преступления, предусмотренного ст. 273 УК РФ, является специальным и альтернативным: это либо компьютерная программа, либо иная компьютерная информация, обладающие признаком вредоносности. Ключевые разъяснения относительно того, что следует понимать под «иной» компьютерной информацией, содержит п. 8 постановления Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37. К иной компьютерной информации, заведомо предназначенной для несанкционированных блокирования, модификации, копирования компьютерной информации или нейтрализации средств ее защиты, могут быть отнесены любые сведения, которые, не являясь в совокупности компьютерной программой, позволяют обеспечить достижение указанных целей. В качестве примера приводятся ключи доступа, позволяющие нейтрализовать защиту компьютерной информации, а также элементы кодов компьютерных программ, способных скрытно уничтожать и копировать информацию.

Доктринальная позиция дополняет законодательный подход. Так, Е.В. Лошенкова обращает внимание на важный момент: вредоносный потенциал реализуется не сам по себе, а через воздействие на работающие полезные коды, где информация выступает катализатором деструктивного процесса. Классическим примером являются эксплойты, то есть собой набор данных, которые заставляют программу работать в несвойственном ей деструктивном режиме[147]. В свою очередь, А.И. Коробеев и А.И. Ролик делают акцент на функциональной характеристике явления: иную вредоносную информацию определяют через ее способность негативно влиять на целостность и доступность компьютерных сведений, притом, что качество программы у нее отсутствует, что позволяет отграничить такую информацию от полноценного вредоносного программного обеспечения[148]. Тот же подход развивает А.Н. Попов, который указывает на целевое предназначение такой информации, где она должна быть специально создана или приспособлена для совершения несанкционированных действий, будь

---

[147] См.: Уголовное право. Особенная часть: учебник для бакалавров / под ред. А. И. Чучаева. 3-е изд., перераб. и доп. С. 407.

[148] См.: Уголовное право Российской Федерации. Особенная часть: учебник / под ред. проф. Л. В. Иногамовой-Хегай. 3-е изд., перераб. и доп. М., 2026. С. 287.

то уничтожение, блокирование, модификация, копирование информации либо нейтрализация средств защиты; при этом автор допускает, что речь может идти как о файлах, так и о специальных программах, хотя и границы предмета несколько расширяются, но сохраняет главный критерий – направленность на деструктивное воздействие[149]. Наиболее системный анализ предлагает А.А. Энгельгардт, формулирующий исчерпывающий перечень признаков компьютерной информации как предмета преступления по ст. 273 УК РФ.

К таким признакам относятся:

1) форма существования в виде сведений или данных;

2) представление в форме электрических сигналов;

3) независимость от средств хранения, обработки и передачи; выражение в виде компьютерной программы либо иной компьютерной информации;

4) заведомая предназначенность для деструктивных действий;

5) отсутствие необходимой санкции на использование.

Особую ценность представляет вывод в том, что отсутствие хотя бы одного из указанных признаков исключает возможность квалификации деяния по ст. 273 УК РФ. В качестве иллюстрации приводится ситуация, когда уничтожение или блокирование информации выступает побочным эффектом нецелевого использования программы, что не образует состава данного преступления[150].

Важно отметить, что анализ правоприменительной практики, где в качестве предмета ст. 273 УК РФ является иная вредоносная компьютерная информация, встречаются значительно реже.

Однако яркой иллюстрацией выступает приговор Бердского городского суда Новосибирской области от 10 ноября 2025 г. по делу № 1-225/2025 в отношении Г.А.С.[151] Из материалов дела следует, что подсудимый, действуя из корыстных

---

[149] Уголовное право России. Особенная часть: учебник / под ред. В. Н. Бурлакова, В.В. Векленко, В.Ф. Щепелькова. 4-е изд., доп. СПб., 2022. С. 653

[150] См.: Энгельгардт А.А. Компьютерная информация как предмет преступления, предусмотренного статьей 273 Уголовного кодекса Российской Федерации // Право. Журнал Высшей школы экономики. 2014. № 4. С. 143.

[151] Приговор Бердского городского суда Новосибирской области от 10 ноября 2025 г. по делу № 1-225/2025 [Электронный ресурс]. – Доступ из СПС «Гарант».

побуждений, создавал и распространял файлы с расширением «*.bd», содержащие программный код для проверки авторизационных данных на интернет-ресурсах. Суд квалифицировал его действия по ч. 2 ст. 273 УК РФ именно как создание и распространение иной компьютерной информации, заведомо предназначенной для несанкционированного уничтожения, модификации, копирования компьютерной информации и нейтрализации средств ее защиты. Примечательно, что орудиями преступления выступили персональный компьютер и мобильный телефон, а полученный преступный доход был конфискован.

Данный приговор является подтверждением согласованности доктринальной позиции относительно понимания иной компьютерной информации. По сути, приговор отражает, что предметом преступления могут быть не только программы, но и отдельные файлы, которые содержат вредоносный код.

Нормативно-правовой анализ Кыргызской Республики демонстрируют нам эволюцию понимания информации от базовых (начальных) формулировок к высокотехнологичным определениям. На протяжении долгого времени специализированные законы выступали основой, которые создали терминологическую базу.

Одним из таких является Закон Кыргызской Республики от 19 июля 2017 г. № 127 «Об электронном управлении» в п. 1 ст. 2, который определяет информацию максимально широко как сведения, сообщения или данные, независимо от формы их представления, что позволяло охватывать любые формы коммуникации и фиксации сведений[152]. Закон Кыргызской Республики от 14 апреля 2008 г. № 58 «Об информации персонального характера»[153] в ст. 3 конкретизировал понятие информации как сведения, зафиксированные на материальном носителе и позволяющие идентифицировать человека, а также вводил важнейшее понятие обработки персональных данных, под которой понимался любой набор операций,

---

[152] Закон Кыргызской Республики от 19 июля 2017 года № 127 «Об электронном управлении» // Газета «Эркин-Тоо». 2017. 25 июля. № 127. URL: https://cbd.minjust.gov.kg/111634/edition/36815/ru (дата обращения: 20.02.2026).

[153] Закон Кыргызской Республики от 14 апреля 2008 года № 58 «Об информации персонального характера» // Газета «Эркин-Тоо». 2008. 18 апр. № 4029. URL: https://cbd.minjust.gov.kg/4-3703/edition/1239270/ru (дата обращения: 20.02.2026).

включая блокирование, стирание и уничтожение, что напрямую коррелирует с действиями, запрещенными уголовным законом. В ст. 2 Закона КР от 19 июля 2017 г. № 128 «Об электронной подписи»[154] оперировал понятиями электронной подписи как информации в электронной форме и ключа подписи как уникальной последовательности символов, что уже тогда позволяло рассматривать эти объекты как потенциальные предметы посягательств, не являющиеся программами в классическом смысле. Однако все эти законы, согласно Закону КР от 31 июля 2025 г. № 179, утрачивают свою силу, уступая место новому, системообразующему акту – Цифровому кодексу Кыргызской Республики[155].

В настоящее время, именно Цифровой кодекс КР формирует современную понятийную матрицу. В п. 98 ст. 1 ЦК КР закреплено базовое понятие «цифровые данные», под которыми понимаются данные, пригодные для обработки с использованием цифровых устройств, независимо от формы и способа их хранения и передачи. Это наиболее широкая категория, охватывающая любые объекты в цифровой среде, будь то программы, тексты, изображения или базы данных, и именно она должна рассматриваться как аналог «компьютерной информации» в контексте уголовно-правовой охраны.

Далее Цифровой кодекс КР производит важную дифференциацию. В п. 20 ст. 1 ЦК КР раскрывается понятие «информации», под которой понимается содержание или контент цифровых данных и цифровых записей, непосредственно доступных для восприятия человеком. Это разграничение принципиально: цифровые данные существуют объективно, как набор сигналов, а информация – это их осмысленное наполнение, то, что мы видим на экране или слышим. Для уголовного права это означает, что предметом преступления могут выступать оба этих уровня – например, вредоносная программа воздействует на цифровые

---

[154] Закон Кыргызской Республики от 19 июля 2017 г. № 128 «Об электронной подписи» // Газета «Эркин-Тоо». 2017. 25 июля. № 128. URL: https://cbd.minjust.gov.kg/4-2446/edition/985628/ru (дата обращения: 20.02.2026).

[155] Закон Кыргызской Республики от 31 июля 2025 года № 179 «О введении в действие Цифрового кодекса Кыргызской Республики» // Газета «Эркин-Тоо». 2025. 5 авг. № 195. URL: https://cbd.minjust.gov.kg/4-5604/edition/35394/ru (дата обращения: 20.02.2026).

данные, а результатом такого воздействия становится уничтожение или модификация информации, воспринимаемой пользователем.

Пункт 32 ст. 1 ЦК КР вводит понятие «метаданных» как структурированных цифровых данных, характеризующих любые цифровые объекты для их идентификации, поиска и управления. Метаданные могут стать самостоятельным предметом посягательства, например, при их фальсификации для сокрытия следов преступления или дезорганизации работы системы.

Крайне важным представляется определение «ключа» в п. 25 ст. 1 ЦК КР как любой информации (кода или шифра), имеющейся у лица и однозначно связывающей его с используемым идентификатором.

Применительно к ст. 320 УК КР, несмотря на отсутствие прямого аналога категории «иной компьютерной информации», развитие цифрового законодательства республики создает предпосылки для расширительного толкования предмета преступления и включения в него, помимо программ, также ключей, смарт-контрактов или иных цифровых записей, способных причинить вред охраняемым отношениям. Дальнейшее развитие уголовно-правовых норм КР видится в направлении конкретизации признаков вредоносных цифровых объектов с учетом современных технологических реалий.

Таким образом, соотношение компьютерной информации и иной вредоносной компьютерной информации в контексте ст. 273 УК РФ следует понимать, как соотношение общего и специального[156].

Компьютерная информация в широком смысле – это любые сведения в электронной форме. В контексте ст. 273 УК РФ иная вредоносная компьютерная информация – это особая разновидность таких сведений, которая, не являясь программой, обладает деструктивным потенциалом и предназначена для совершения несанкционированных действий.

Пожалуй, в ракурсе ст. 320 УК КР иная вредоносная компьютерная информация представляет собой любые цифровые данные (ключи, метаданные,

---

[156] Приложение № 3 «Терминологическая модель исследования» к диссертации.

части кода, скрипты), которые, не являясь самостоятельной программой в традиционном смысле, созданы для несанкционированного воздействия на цифровую среду или нейтрализации ее защиты.

И в завершение данного параграфа следует указать на следующее. Российскому уголовному законодательству характерно специальное определение основания ответственности за совершение действий с вредоносными компьютерными программами, заведомо предназначенными для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации (ч. 1 ст. 274^1 УК РФ). Вопрос о правовой сущности и технологической уникальности таких программ отдельно не раскрывался по той простой причине, что, как и многие другие авторы[157], мы полагаем, что такую специальную предназначенность для совершения воздействия именно на информационную инфраструктуру критической важности установить невозможно. В настоящее время практика по ч. 1 ст. 274^1 УК РФ строится преимущественно на случаях, когда вредоносные компьютерные программы фактически применялись и были эффективны в отношении критической инфраструктуры. При этом изучение судебных решений в части описания выводов проведенных компьютерных экспертиз не позволяет выявить примеры, где бы технический специалист указывал на уникальность таких программ именно для атак в отношении КИИ. Как правило, это те же самые вредоносные компьютерные программы (либо обладающие сходной архитектурой и функционалом), которые встречаются и в обвинительных приговорах и по ст. 273 УК РФ.

[157] См., например: Дремлюга Р. И., Зотов С. С., Павлинская В. Ю. Критическая информационная инфраструктура как предмет преступного посягательства // Азиатско-Тихоокеанский регион: экономика, политика, право. 2019. Т. 21. № 2. С. 136.

§ 2. Объективная сторона создания, использования и распространения вредоносных компьютерных программ (ст. 273 УК РФ, ст. 320 УК КР)

В доктрине уголовного права, по единодушному мнению ученых-правоведов, объективная сторона преступления имеет фундаментальное значение. Как отмечает А.Н. Попов, ее четкое закрепление в законе позволяет принимать верные уголовно-правовые решения[158]. А.И. Чучаев выделяет несколько аспектов: установление состава преступления, квалификация, отграничение от иных правонарушений и значение для наказания[159]. Л.М. Прохорова добавляет, что она является основанием уголовной ответственности, позволяет установить направленность умысла и разграничить сходные составы[160]. Таким образом, объективная сторона – ключевой элемент для квалификации и правоприменения.

Объективная сторона преступления, предусмотренного ст. 273 УК РФ, выражается в трех альтернативных действиях, а именно: создание, распространение или использование вредоносных компьютерных программ либо иной вредоносной компьютерной информации. В отличие от российской нормы, диспозиция ст. 320 УК КР охватывает не только создание, распространение или использование, но также внесение изменений в существующий программный продукт. Соответственно, объективная сторона преступления, предусмотренная ст. 320 УК КР, состоит из четырех альтернативных действий.

Начнем с формы общественного опасного действия – создание вредоносных компьютерных программ или программного продукта, которое предусмотрено ст. 273 УК РФ и ст. 320 УК КР. Содержание этого признака комплексное и меняется

---

[158] См.: Арзамасцев М. И., Бойцов А. И., Бурлаков В. Н. и др. Уголовное право России. Общая часть: учебник / под ред. В. В. Лукьянова, В. С. Прохорова, В. Ф. Щепелькова, 3-е изд. перераб. и доп.СПб., 2013. С. 155.

[159] См.: Грачева Ю. В., Чучаев А. И. Уголовное право России. Общая и особенная части: учебник. М., 2017. С. 49.

[160] См.: Российское уголовное право. Общая часть: учебник / под ред. В. П. Коняхина. М., 2016. С. 187.

вместе с развитием цифровых технологий, а следовательно отражается в расширительном толковании его сущности.

Согласно позиции п. 9 Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37 создание представляет собой деятельность, направленную на разработку или подготовку вредоносных программ (включая модификацию существующих) либо иной компьютерной информации[161]. Ключевым критерием является их изначальная предназначенность для совершения несанкционированных действий, таких как уничтожение, блокирование, модификация, копирование информации или нейтрализация средств ее защиты. Настоящее определение подчеркивает, что важен сам факт целенаправленной разработки вредоносного продукта, при этом не имеет значение были программа окончательно доработана и применена на практике.

Аналогичный подход демонстрируют и Методические рекомендации по осуществлению прокурорского надзора, акцентирующие внимание на разработке программ с деструктивным функционалом[162].

Содержание признака «создание» более детально и углублено рассматривается в доктрине уголовного права. Так, Е.А. Русскевич[163] и А.Г. Кибальник[164] определяют создание как целенаправленную деятельность, результатом которой является появление программного продукта с заранее заданными вредоносными свойствами. Как справедливо отмечают ученые, при создании вредоносного программного обеспечения не требуется от лица особо

---

[161] О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»: постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 // СПС «Консультантлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_434573/ . (дата обращения: 06.09.2025).

[162] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации. М.: Генеральная Прокуратура РФ. 2013. URL: https://epp.genproc.gov.ru/web/gprf/documents (дата обращения: 06.09.2025).

[163] См.: Калиниченко И. А., Андреев А. В., Галиев Д. В. и др. Противодействие преступлениям в сфере информационных технологий : учебник / под науч. ред. И. А. Калиниченко ; под техн. ред. В. В. Гончара. С. 147.

[164] См.: Уголовное право. Особенная часть: учебник для вузов / отв. ред. А. В. Наумов, А. Г. Кибальник. 6-е изд., перераб. и доп. М.: Издательство Юрайт, 2025. С. 388.

профессиональных навыков программирования, тем самым расширяется круг потенциальных субъектов преступления.

Наиболее детализированную структурную декомпозицию признака «создание» предлагает М.Ю. Дворецкий. Он рассматривает его как протяженный во времени процесс, включающий несколько этапов: постановку задачи и определение цели программы, выбор средств и языков программирования, написание непосредственно текста (кода), отладку, а также запуск и тестирование[165]. Исходя из этой позиции, преступление считается оконченным с любого момента из перечисленных этапов, даже если вредоносная программа не была доведена до полной готовности к применению. Следовательно, это означает, что уголовная ответственность по ст. 273 УК РФ может наступать на стадии подготовки.

С.М. Корабельников[166] и Е.А. Маслакова[167] акцентируют внимание на результате деятельности – появлении объективно выраженного комплекса данных и команд, предназначенного для функционирования в компьютерных устройствах и обладающего деструктивным потенциалом. К.Н. Евдокимов развивает эту мысль, указывая, что создание охватывает не только разработку «с нуля», но и любую модификацию уже существующих программ в целях придания или усиления их вредоносных свойств. Он также определяет важный критерий окончания преступления – момент, когда программа приобретает вредоносные свойства и готова к использованию[168]. Это позволяет разграничить этап приготовления и оконченное преступление.

Проведенный анализ позволяет сделать вывод о том, что признак «создание» в ст. 273 УК РФ интерпретируется максимально широко. Он включает в себя как

---

[165] См.: Дворецкий М.Ю. Преступления в сфере компьютерной информации: понятие, система, проблемы квалификации и наказания [Текст]: монография / М.Ю. Дворецкий. Тамбов, 2003. С. 79.

[166] См.: Корабельников С.М. Указ соч. С. 78.

[167] См.: Маслакова Е.А. Анализ объективной стороны преступления, связанного с незаконным оборотом вредоносных компьютерных программ // Известия ТулГУ. Экономические и юридические науки. 2008. № 1. С. 229.

[168] См.: Евдокимов К.Н. Противодействие компьютерной преступности: теория, законодательство, практика: дис. ... д-ра юрид. наук. М., 2021. С. 328

полный цикл разработки вредоносной программы, так и отдельные действия по ее модификации или сборке из готовых компонентов, и может считаться оконченным на достаточно ранней стадии – с момента, когда вредоносный продукт начал формироваться и приобрел (или был предназначен для приобретения) деструктивный функционал.

Так, Б.М.И. и О.Л.Ф., действуя группой лиц по предварительному сговору из корыстной заинтересованности, целенаправленно и умышленно осуществляли совместную деятельность по созданию компьютерных программ, заведомо предназначенных для несанкционированного копирования и модификации компьютерной информации, а также для нейтрализации средств защиты антивирусного программного обеспечения АО «Лаборатория Касперского». Процесс создания включал в себя непосредственную разработку Б.М.И. исполняемых файлов (KRT_CLUB_8.0.0.37.exe, KRT_CMD_2.0.0.3.exe, KRT_CLUB_8.1.0.4.exe) с использованием компьютерной техники как по месту жительства, так и на работе, при этом О.Л.Ф. активно участвовал в создании, предоставляя необходимую информацию для включения в код, рекомендации по доработке функционала и пользовательского интерфейса, т.е. их действия были согласованными и направленными именно на создание вредоносного продукта. После создания программ обвиняемые не только использовали их для личных целей, но и организовали их возмездное распространение через специально созданный ими интернет-ресурс, что является продолжением их преступного умысла, исходным и ключевым элементом которого выступает именно факт создания указанных вредоносных программ[169].

В ст. 320 УК КР «создание» не получает законодательного и доктринального определения. Это обусловливает необходимость толкования.

По смыслу кыргызской статьи «создание» представляет собой полный или частичный цикл действий по разработке вредоносного программного продукта. При этом, стоит обратить внимание, что при «создании» обязательным признака

[169] Приговор Выксунского городского суда Нижегородской области от 27 мая 2024 г. по делу № 1-139/2024 [Электронный ресурс]. – Доступ из СПС «Гарант».

субъективной стороны является наличие специальной цели использования или распространение, предусмотренного ст. 320 УК КР. В данном случае, создание не требует обязательного доведения программы до полной готовности, но важно установить, что виновный преследовал указанную цель при разработке вредоносного программного продукта.

Анализ доктринального толкования такого действия как «использование», предусмотренного ст. 273 УК РФ и ст. 320 УК КР демонстрирует близость подходов, но и определенную специфику аккцентов, а также степень детализации.

Пленум Верховного Суда РФ в своем постановлении[170] задает ключевой вектор, согласно которому использование понимается как применение программ или информации, в результате которого происходит умышленное уничтожение, блокирование, модификация, копирование компьютерной информации или нейтрализация средств ее защиты. Важным уточнением является указание на то, что не образует состава преступления использование на принадлежащих лицу устройствах или с согласия собственника, если оно не преследует противоправных целей и не влечет вредоносных последствий, например, в образовательных или тестовых целях.

В российской уголовной доктрине сложилось единое понимание относительно того, что использование подразумевает применение, который приводит к активизации заложенного вредоносного функционала. Так, В.А. Авдеев определяет его как введение в оборот или применение по основному назначению, то есть акцентируя тем самым функциональный аспект[171]. В.Ю. Максимов[172] и М.М. Малыковцев[173] рассматривают более детализировано,

---

[170] 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”».

[171] См.: Уголовное право России. Части Общая и Особенная: учебник для бакалавров / отв. ред. А. И. Рарог. 2-е изд., перераб. и доп. М., 2020. С. 536.

[172] См.: Максимов В.Ю. Незаконное обращение с вредоносными программами для ЭВМ : Проблемы криминализации, дифференциации ответственности и индивидуализации наказания: дис. ... канд. юрид. наук. Краснодар, 1998. С. 100.

[173] См.: Малыковцев М.М. Указ. соч. С. 90–91.

указывая, что момент использования напрямую зависит от свойств самой программы: для программ с немедленным действием он наступает с момента запуска, а для «логических бомб» или «закладок» – с момента срабатывания. Эта позиция подчеркивает необходимость учета технических особенностей вредоносного программного обеспечения при квалификации. А.И. Коробеев делает акцент на цели действия, сводя использование к внедрению в информационный оборот для реализации вредоносных качеств[174].

Схожим образом М.А. Простосердов[175] определяет использование как применение программы по назначению, приводящее к активизации ее вредоносных свойств.

Более узкое, техническое определение предлагает М.А. Ефремова, понимая под использованием просто запуск программы в компьютере[176].

В.Б. Боровиков[177] и В.В. Сверчков[178] фокусируются на результате, определяя использование как достижение преступного последствия (несанкционированного уничтожения, блокирования и т.д.) или как запуск и эксплуатацию в компьютерных системах. Таким образом, российская доктрина в целом трактует использование как действие по применению программы, которое приводит к реализации ее деструктивного потенциала, причем ключевое значение имеет не сам факт запуска, а наступление вредоносных последствий или как минимум создание реальной угрозы их наступления.

Так, например, по одному из дел суд указывает, что подсудимый, обладая специальными познаниями в области информационных технологий, предварительно изучил в сети «Интернет» инструкции по применению

---

[174] См.: Иногамова-Хегай Л.В. Уголовное право Российской Федерации. Особенная часть: учебник / под ред. проф. Л. В. Иногамовой-Хегай. 3-е изд., перераб. и доп. С. 288.

[175] См.: Андрианов В.К., Арямов А.А., Блинников В.А. и др. Уголовное право России. Части Общая и Особенная: учебник / под ред. А. В. Бриллиантова. 3-е изд., перераб. и доп. М., 2021. С. 1004.

[176] См.: Ефремова М.А. Уголовная ответственность за преступления, совершаемые с использованием информационно-телекоммуникационных технологий. М., 2015. С. 104.

[177] См.: Боровиков В.Б., Смердов А.А. Уголовное право. Особенная часть: учебник для вузов / под ред. В. Б. Боровикова. 7-е изд., перераб. и доп. М., 2025. С. 275.

[178] См.: Сверчков В.В. Уголовное право. Особенная часть: учебник для вузов. 12-е изд., перераб. и доп. М., 2025. С. 330.

вредоносного программного обеспечения, после чего загрузил на свой персональный компьютер программу “sqlmap”, а также иные вредоносные программы, заведомо предназначенные для несанкционированного копирования информации, в частности логинов и паролей пользователей, хранящейся на различных интернет-ресурсах. В установленный период, находясь по месту жительства и используя предоставленный провайдером доступ к сети «Интернет», он применил указанные программы для осуществления несанкционированного доступа и незаконного воздействия на информационные ресурсы, что было подтверждено заключением программно-технической экспертизы, идентифицировавшей как сами вредоносные объекты, так и следы их целенаправленного использования против конкретных интернет-ресурсов. Таким образом, суд квалифицировал его действия именно как использование вредоносных программ для несанкционированного копирования компьютерной информации, что полностью соответствует диспозиции ч. 1 ст. 273 УК РФ[179].

В сравнительном аспекте доктринальное толкование ст. 320 УК Кыргызской Республики демонстрирует более лаконичный подход. З.К. Курманов и Р.А. Окенова определяют использование через его цель – несанкционированное уничтожение, блокирование, модификацию либо копирование информации, нарушение работы компьютерной системы[180]. К.М. Осмоналиев дает еще более краткое определение – применение программы при работе на ЭВМ[181]. Несмотря на сходство с российской доктриной в понимании сути деяния, кыргызские подходы в меньшей степени детализируют механизм и момент совершения использования, фокусируясь на его целевой направленности или самом факте применения.

В результате проведенного анализа можно сделать вывод о высокой степени унификации понимания «использования» вредоносных программ в уголовном

---

[179] Приговор Нефтеюганского районного суда Ханты-Мансийского автономного округа Югры от 22 апреля 2019 г. по делу № 1-187/2019 [Электронный ресурс]. – Доступ из СПС «Гарант».
[180] См.: Курманов К.Ш. Указ. соч. С. 397.
[181] См.: Осмоналиев К.М. Уголовное право Кыргызской Республики (Особенная часть) : учеб. пособие / под общ. ред. проф. В. П. Ревина. – 2-е изд. Бишкек, 2005. С. 217.

праве России и Кыргызстана. Российская доктрина и судебная практика, опираясь на разъяснения, содержащиеся в постановлении Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37, выработали более развернутое и технологически ориентированное определение, которое учитывает различные модели поведения злоумышленника и типы вредоносных программ. Оба правовых порядка сходятся в том, что ядром использования является активное действие по применению программы, приводящее к реализации ее вредоносных функций и наступлению общественно опасных последствий.

В соответствии со ст. 273 УК РФ и ст. 320 УК КР третьим видом общественно опасного действия объективной стороны преступления является «распространение». Определение, закрепленное в постановлении Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37[182], а также в Методических рекомендациях Генеральной прокуратуры Российской Федерации[183], дает широкий спектр форм, согласно которому распространение понимается как предоставление доступа к вредоносным программам или информации конкретным лицам либо неопределенному кругу лиц любым способом. К этому числу способов относятся передача на электронном носителе, продажа, рассылка, то есть законодатель старается максимально возможные каналы распространения.

В российской доктрине уголовного права демострируется общее понимание сущности распространения. Большинство авторов, включая В.А. Авдеева[184],

---

[182] О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»: постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 // СПС «Консультантлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_434573/ . (дата обращения: 06.09.2025).

[183] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации. М.: Генеральная Прокуратура РФ. 2013. URL: https://epp.genproc.gov.ru/web/gprf/documents (дата обращения: 08.09.2025).

[184] См.: Уголовное право России. Части Общая и Особенная: учебник для бакалавров / отв. ред. А. И. Рарог. С. 536.

М.А. Простосердова[185], В.Б. Боровикова[186], В.В. Сверчкова[187], акцентируют внимание на действиях по предоставлению доступа к программе, ее копированию и введению в оборот. Ключевое значение придается именно факту *предоставление доступа*, а не физической передаче с одного носителя на другой. При этом не имеет значения, каким образом доступ был обеспечен: он может осуществляться как сетевыми методами (через сеть «Интернет»), так и иными – «аналоговыми» способами, то есть передача физических носителей информации.

Особый интерес представляет позиция М.А. Ефремовой[188], которая указывает на возможность распространения путем простой передачи другому лицу, и М.М. Малыковцева, который включает в это понятие даже умышленную рассылку по электронной почте, тем самым расширяя спектр охватываемых действий[189]. Существенным является замечание М.М. Малыковцева о том, что самовоспроизводящийся характер компьютерного вируса не исключает ответственности лица, которое своими активными действиями (продажа, рассылка) инициировало его распространение. А.И. Коробеев[190] и И.А. Ефремова[191] делают акцент на аспекте отчуждения программы или информации, что сближает распространение с понятием обращения объекта в гражданском обороте, но с противоправной целью.

В контексте настоящего исследования особый интерес вызывает судебный акт по делу о распространении вредоносной программы через публичный канал в мессенджере Telegram. В приговоре Прохладненского районного суда Кабардино-Балкарской Республики установлено, что гражданин У., руководствуясь

---

[185] См.: Андрианов В.К., Бриллиантов А.В., Кауфман М.А. и др. Комментарий к Уголовному кодексу Российской Федерации (постатейный): в 2 т. / под ред. А. В. Бриллиантова. 3-е изд., перераб. и доп. М., 2021. С. 354.

[186] См.: Боровиков В.Б., Смердов А.А. Уголовное право. Особенная часть: учебник для вузов / под ред. В.Б. Боровикова. С. 275.

[187] См.: Сверчков В.В. Уголовное право. Особенная часть: учебник для вузов. С. 330.

[188] См.: Ефремова М. А. Уголовная ответственность за преступления, совершаемые с использованием информационно-телекоммуникационных технологий. С. 104.

[189] См.: Малыковцев М. М. Указ. соч. С. 95.

[190] См.: Уголовное право Российской Федерации. Особенная часть: учебник / под ред. проф. Л. В. Иногамовой-Хегай. 3-е изд., перераб. и доп. С. 287.

[191] См.: Ефремова И. А. Уголовное право (Особенная часть): курс лекций / под ред. и с предисл. Б. Т. Разгильдиева. С. 336.

корыстным мотивом и стремлением к извлечению дохода от монетизации созданного им канала, обнаружил в сети Интернет компьютерную программу «HighOrbitlonCannon». Технические характеристики этой программы указывали на ее предназначения для осуществления DDoS-атак и блокирования информации. Гражданин У. осознавал ее вредоносную природу, что в последующим подтвердилось срабатыванием антивирусной защиты, разместил в общедоступном Telegram-канале «RustorStill». Суд квалифицировал эти действия по ч. 2 ст. 273 УК РФ как распространение вредоносной компьютерной программы, заведомо предназначенной для несанкционированного блокирования компьютерной информации, что в полной мере характеризует объективную сторону вмененного деяния[192].

В кыргызской доктрине толкование ст. 320 УК КР демонстрируют практически схожую направленность, но более сжатые формулировки. Так, З.К. Курманов и Р.А. Окенова считают, что под распространением можно считать две основные: с помощью средств компьютерной связи и простую передачу другому лицу[193].

В свою очередь, К. М. Осмоналиев конкретизирует способы, перечисляя продажу, дарение и иные способы предоставления доступа, включая сетевые[194]. Таким образом, хотя кыргызская доктринальная мысль оперирует менее детализированным понятийным аппаратом по сравнению с российской, сущностное содержание деяния понимается аналогично: это *любые действия, направленные на то, чтобы сделать вредоносную программу доступной для других лиц.*

Проведенный анализ демонстрирует нам, что в уголовном праве России и Кыргызстана складывается единый подход в понимании распространения вредоносных программ. Пожалуй, отличие проявляется лишь в степени детализации, то есть в охвате способов, который более проработан в российской

---

[192] Приговор Прохладненского районного суда Кабардино-Балкарской Республики от 23 апреля 2025 г. по делу № 1-161/2025 [Электронный ресурс]. – Доступ из СПС «Гарант».
[193] См.: Курманов К.Ш. Указ. соч. С. 387.
[194] См.: Осмоналиев К.М. Указ. соч. С. 217.

доктрине, чем в кыргызской. Обе правовые системы сходятся в том, что ядром распространения является активное действие виновного, результатом которого становится получение другим лицом (лицами) возможности использовать вредоносную программу. Такой подход обеспечивает адекватное уголовно-правовое реагирование на постоянно эволюционирующие способы совершения компьютерных преступлений.

Одним из ключевых отличий объективной стороны состава преступлений, предусмотренного ст. 320 УК КР, от ст. 273 УК КР является подход к криминализации действий с вредоносными программами. Так, в 2011 г., внося изменения в УК РФ, российский законодатель исключил из перечня общественно опасных деяний по ст. 273 УК РФ такое действие, как «внесение изменений в существующие программы»[195]. Кыргызский законодатель, в отличие от российского, прямо включил в состав такую альтернативную форму, как «внесение изменений в существующие программные продукты», при условии, что они заведомо предназначены для достижения перечисленных в законе последствий.

Думается, что такой подход существенно расширяет сферу уголовно-правового запрета. Это означает, что в соответствии с УК КР уголовная ответственность наступает за сам факт целенаправленного изменения существующей программы, если целью или следствием этого изменения является придание или сохранение у нее свойств, направленных на несанкционированный доступ, уничтожение, блокирование информации и т.д. Таким образом, позиция, высказанная Е.А. Маслаковой применительно к российскому законодательству, о том, что модификация программы является преступной лишь при добавлении или изменении вредоносных функций[196], в рамках ст. 320 УК КР находит прямое законодательное закрепление. Более того, кыргызская норма, по всей видимости, охватывает и ситуацию, описанную М.М. Малыковцевым, когда изменения

---

[195] Федеральный закон от 7 декабря 2011 г. № 420-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» // СЗ РФ. 2011. № 50. Ст. 7362.

[196] См.: Маслакова Е. А. Незаконный оборот вредоносных компьютерных программ: уголовно-правовые и криминологические аспекты : дис. ... канд. юрид. наук. М., 2008. С. 85–86.

вносятся в уже вредоносную программу, но не для ее обезвреживания, а для сохранения или модификации ее деструктивного потенциала, поскольку такие действия подпадают под признак «внесение изменений в существующие программные продукты, заведомо предназначенные для осуществления...»[197] вредоносных действий.

Ключевым критерием в ст. 320 УК КР является «заведомая предназначенность» программного продукта для совершения вредоносных действий. Это позволяет распространить действие нормы на случаи, аналогичные приведенным В.Ю. Максимовым, когда лицо не создает программу заново, а видоизменяет существующий алгоритм, придавая ему иные вредоносные свойства. Такую деятельность логично рассматривать как «внесение изменений» в целях создания качественно новой угрозы[198].

Следовательно, основное отличие заключается в том, что российский законодатель, исключив «внесение изменений» из ст. 273 УК РФ, сделал акцент исключительно на создании, использовании и распространении вредоносных программ. Кыргызский же подход является более широким и детализированным, поскольку он целенаправленно криминализирует модификацию существующего вредоносного программного обеспечения как самостоятельный способ совершения преступления, что позволяет более гибко подходить к квалификации действий злоумышленников, активно использующих методы доработки и адаптации уже существующих кодов для достижения противоправных целей.

Другой отличительный признак объективной стороны составов преступлений, предусмотренных ст. 273 УК РФ и ст. 320 УК КР, выражается в конструкции составов.

На протяжении всех редакций сохраняется формальный тип состава, предусмотренного ст. 273 УК РФ, что подтверждается анализом эволюции настоящей статьи.

---

[197] Малыковцев М.М. Указ. соч. С. 87.
[198] См.: Максимов В.Ю. Указ. соч. С. 98.

Как справедливо отмечает М.М. Малыковцев, отнесение деяния к преступлениям с формальным составом обусловлено высокой степенью общественной опасности самого факта создания или оборота вредоносных программ, что делает излишним для квалификации преступления обязательное наступление реальных общественно опасных последствий[199]. Эта фундаментальная позиция, сформировавшаяся в доктрине еще на этапе действия ранних редакций статьи, впоследствии получила подтверждение и развитие в трудах современных ученых. Так, большинство ученых едины во мнении, что основной состав ч. 1 ст. 273 УК РФ сконструирован как формальный[200]. Это означает, что преступление считается оконченным с момента совершения любого из указанных в диспозиции действий – создания, распространения или использования вредоносных программ, независимо от того, повлекли ли они фактическое уничтожение, блокирование, модификацию или копирование информации.

По мнению И.Р. Бегишева, отсутствует необходимость доказывания причинно-следственной связи между деянием и наступившем последствием, в связи с достаточным фактом совершения действий, предусмотренных ст. 273 УК РФ[201]. В дополнение к этой позиции, можно привести мнение М.А. Ефремовой, которая считает, что такой законодательный подход позволяет эффективно противодействовать рассматриваемым угрозам на ранней стадии, не дожидаясь реализации деструктивного потенциала вредоносных программ[202].

Что касается квалифицированных составов, представленных в ч. 2 и 3 действующей редакции ст. 273 УК РФ, то здесь конструкция усложняется. В ч. 2 ст. 273 УК РФ содержатся как признаки, свойственные формальному составу

---

[199] Малыковцев М.М. Указ. соч. С. 79.

[200] Евдокимов К.Н. Противодействие компьютерной преступности: теория, законодательство, практика: дис. ... д-ра юрид. наук. М., 2021. С. 298; Ефремова М.А. Уголовно-правовая охрана информационной безопасности: дис. ... д-ра юрид. наук. М., 2017. С. 180; Русскевич Е.А. Дифференциация ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий, и проблемы их квалификации: дис. ... д-ра юрид. наук. М., 2021. С. 294.

[201] См.: Бегишев И.Р. Указ. соч. С. 66.

[202] См.: Ефремова М.А. Уголовно-правовая охрана информационной безопасности: дис. ... д-ра юрид. наук. М., 2017. С. 350.

(совершение деяния группой лиц по предварительному сговору, организованной группой, лицом с использованием своего служебного положения, а также из корыстной заинтересованности), так и признак, переводящий его в категорию материальных – причинение крупного ущерба. Крупный ущерб, определяемый в соответствии с примечанием к ст. 272 УК РФ как сумма, превышающая один миллион рублей, представляет собой общественно опасное последствие.

Если деяние квалифицируется по ч. 2 ст. 273 УК РФ по признаку причинения крупного ущерба, то для оконченного состава преступления необходимо установить не только само действие (создание, использование, распространение), но и наступление этого конкретного последствия, что характерно для материального состава. В ч. 3 ст. 273 УК РФ установлена ответственность за деяния, повлекшие тяжкие последствия или создавшие угрозу их наступления. Данный состав является формально-материальным, поскольку преступление считается оконченным как с момента фактического наступления тяжких последствий (материальный признак), так и с момента создания реальной угрозы их наступления (формальный признак). Эволюция настоящего подхода демонстрирует движение законодателя от простого формального состава к более сложной смешанной конструкции.

Существенная трансформация юридической конструкции наблюдается и в уголовном законодательстве Кыргызской Республики, которая заключается в переходе от формального к материальному составу. В первоначальной редакции УК КР 1997 г. (ст. 290) и в последующей редакции УК КР (ст. 305), которая позднее утратила силу[203], состав преступления был сконструирован как формальный, что является классическим подходом для данного вида деяний. Преступление считалось оконченным с момента совершения самих действий по созданию, использованию или распространению вредоносных программ, независимо от наступления каких-либо реальных вредных последствий. Эта модель, аналогичная

[203] Уголовный кодекс Кыргызской Республики от 2 февраля 2017 г. № 19: утратил силу в соответствии с Законом Кыргызской Республики от 28 октября 2021 г. № 126. URL : https://cbd.minjust.gov.kg/111527/edition/1186183/ru (дата обращения: 22.09.2025).

ранней редакции ст. 273 УК РФ, была направлена на пресечение самой возможности оборота опасных программ на максимально ранней стадии.

Последующее реформирование уголовного закона привело к кардинальному изменению подхода. В действующей редакции УК КР 2021 г. в случае создания вредоносного программного продукта или внесения изменения в существующий вредоносный программный продукт наступление последствий не является обязательным признаком для привлечения к уголовной ответственности, что говорит о формальной конструкции состава по отношению к этим формам действий, в ситуации с использованием или распространением вредоносного программного продукта, законодатель указал на необходимость наступления последствий в ч. 1 ст. 320 УК КР в виде причинения *значительного ущерба*.

Необходимо подчеркнуть, что гл. 40 УК КР не содержит специальных примечаний, разъясняющих содержание последствий. В связи с этим для правильной квалификации деяния по ч. 1 ст. 320 УК КР принципиальное значение имеет определение, закрепленное в п. 6 Приложения 1 к УК КР, согласно которому значительный ущерб как материальный (имущественный) ущерб исчисляется в размере, превышающем в 100 раз расчетный показатель, установленный на момент преступления.

Однако, как справедливо отмечает Л.Ч. Сыдыкова, преступления, предусмотренные гл. 40 УК КР, зачастую влекут и нематериальные последствия, что требует глубокого научного осмысления[204]. Ученый разграничивает категории «вред» (более широкое понятие) и «ущерб» (связан с имущественными потерями)[205]. В контексте ст. 320 УК КР это означает, что значительный ущерб может выражаться не только в порче оборудования, но и в затратах на восстановление баз данных, утрате информации или остановке производства, что в итоге поддается стоимостной оценке.

---

[204] См.: Сыдыкова Л.Ч. Указ. соч. Уголовное право Кыргызской Республики. Общая часть. Преступление. Наказание: учебник. Бишкек : Издательский дом КРСУ, 2023. С. 183.
[205] Там же. С. 185.

Поскольку доктринальное осмысление этих вопросов в Кыргызстане только формируется, представляется необходимым собственное толкование. Под причинением значительного ущерба по смыслу ст. 320 УК КР следует понимать последствия неправомерного распространения или использования программного продукта, которые охватывают как реальные убытки, так и упущенную выгоду потерпевшего, подтвержденные документально (например, затраты на восстановление системы или ремонт оборудования), и при этом сумма таких убытков превышает 100 расчетных показателей. При отсутствии такого материального выражения последствий либо при недоказанности размера ущерба деяние не образует состава преступления по ч. 1 ст. 320 УК КР.

Это означает, что в настоящее время состав является формально-материальным и уголовная ответственность за использование или распространение вредоносного программного продукта наступает не с момента совершения действий, а лишь при условии фактического наступления указанных последствий. Такая конструкция существенно сужает сферу уголовно-правового реагирования по сравнению с предыдущими редакциями. При этом квалифицированные составы, предусмотренные ч. 2 ст. 320 УК КР, сохраняют также формально-материальную конструкцию, ужесточая наказание за те же деяния, но совершенные при отягчающих обстоятельствах, таких как совершение группой лиц или причинение по неосторожности крупного ущерба, в том числе в отношении критической информационной инфраструктуры.

Сравнительный анализ, проведенный в § 3 гл. 1, показывает нам, что кыргызская модель с материальным составом в части использования и распространения в странах СНГ является скорее исключением, тогда как большинство государств, включая Россию, Казахстан, Таджикистан, Узбекистан и Армению, придерживаются формальной конструкции основного состава. Это расхождение имеет не только доктринальное, но и практическое значение, поскольку существенно сужает возможности раннего пресечения преступной деятельности в Кыргызской Республике по сравнению с Российской Федерацией.

Таким образом, современный кыргызский законодатель признает создание вредоносных программ и внесение изменений в существующие вредоносные программы общественно опасным деянием, но в отличие от российского законодателя подход к их последующему введению в оборот (использованию и распространению) в Кыргызстане является более узким, что может создавать дополнительные процессуальные барьеры для правоприменения по сравнению с более широкими рамками формального состава, принятыми в России.

§ 3. Субъективные признаки создания, использования и распространения вредоносных компьютерных программ (ст. 273 УК РФ, ст. 320 УК КР)

Традиционно в доктрине уголовного права под субъективной стороной преступления следует считать психическую деятельность лица, связанную с совершением преступления, образующую его внутреннее содержание и познаваемую через анализ поведения. Ее юридическое значение состоит в том, что она отграничивает преступное от непреступного, позволяет различать сходные составы и влияет на степень общественной опасности деяния и меру наказания[206]. Следовательно, элементом состава любого преступления является его субъективная сторона, которая раскрывает внутреннее, психическое отношение лица к совершаемому деянию и его последствиям. В российской доктрине существует устоявшееся понимание субъективной стороны преступления.

В доктрине уголовного права Кыргызской Республики субъективная сторона также понимается как психическое отношение лица к совершенному преступлению, характеризуемое конкретной формой вины, мотивом и целью, и рассматривается в качестве внутренней сущности преступления, в противовес его внешней картине, образуемой объективной стороной[207].

---

[206] См.: Уголовное право России. Части Общая и Особенная: учебник для бакалавров / отв. ред. А. И. Рарог. 2-е изд., перераб. и доп. С. 89–90.

[207] См.: Сыдыкова, Л. Ч. Уголовное право Кыргызской Республики. Общая часть. Преступление. Наказание: учебник. Бишкек : Издательский дом КРСУ, 2023. С. 210.

Несмотря на то что субъективная сторона не всегда поддается прямой и достоверной фиксации, однако она проявляется в объективной действительности. Ее установление является обязательным условием правильной квалификации содеянного и отграничения преступного поведения от непреступного. В связи с этим комплексное исследование субъективных признаков преступлений, предусмотренных ст. 273 УК РФ и ст. 320 УК КР, приобретает особую актуальность, поскольку позволяет выявить как общие, так и специфические черты психического отношения виновного к деянию в схожих по объекту посягательства составах преступлений в смежных правовых системах.

Переходя к анализу субъективных признаков состава преступления, предусмотренного ст. 273 УК РФ, следует отметить, что в отечественной доктрине уголовного права по данному вопросу сформировалась достаточно единая позиция. Подавляющее большинство ученых сходится во мнении, что субъективная сторона данного деяния характеризуется виной исключительно в форме прямого умысла. Так, А.Н. Попов указывает, что виновный осознает общественную опасность своих действий, а именно то, что он создает, использует или распространяет программы или файлы, которые заведомо для него обладают функционалом (качествами) оказания несанкционированного воздействия на охраняемую законом компьютерную информацию, и именно этого он желает[208].

Аналогичную точку зрения развивает М.А. Простосердов, подчеркивая, что лицо не просто осознает факт создания или распространения программ, но и понимает их специальную предназначенность для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств ее защиты, и желает совершить такие деяния[209]. Эта мысль находит поддержку и в работах других авторов. В.Б. Боровиков[210] также однозначно характеризует субъективную сторону

---

[208] См.: Уголовное право России. Особенная часть: учебник / под ред. В. Н. Бурлакова, В. В. Векленко, В. Ф. Щепелькова. 4-е изд., доп. С. 654.

[209] См.: Андрианов В. К., Арямов А.А., Блинников В. А. и др. Уголовное право России. Части Общая и Особенная: учебник / под ред. А. В. Бриллиантова. 3-е изд., перераб. и доп. С. 1004.

[210] См.: Боровиков В.Б., Смердов А.А. Уголовное право. Особенная часть: учебник для вузов / под ред. В. Б. Боровикова. 7-е изд., перераб. и доп. С. 276.

исследуемого преступления прямым умыслом, не допуская иной формы вины для основного состава преступления.

Важным представляется уточнение, которое вносит А.Р. Нагайев, акцентируя внимание на законодательном термине «заведомо». Этот термин, по его мнению, означает, что виновный заранее, до совершения действий, осознает факт возможности незаконного использования создаваемых или распространяемых программ для нарушения целостности, конфиденциальности или доступности чужой компьютерной информации. Особый интерес представляет позиция В.В. Сверчкова, который, соглашаясь с господствующим подходом о прямом умысле для основного состава, обращает внимание на квалифицированные составы, предусмотренные ч. 2 и 3 ст. 273 УК РФ[211]. Он указывает, что в случаях, когда в результате совершения данного преступления по неосторожности наступают тяжкие последствия в виде крупного ущерба или иного общественно опасного вреда, речь должна идти о преступлении с двумя формами вины.

Таким образом, в целом субъективная сторона преступления, предусмотренного ст. 273 УК РФ, в ее основном составе понимается учеными как прямой умысел, при котором виновный осознает общественную опасность своих действий и желает их совершения.

В апелляционном определении по делу Александрова Судебная коллегия Московского городского суда рассмотрела вопросы субъективной стороны преступления, предусмотренного ч. 2 ст. 273 УК РФ[212]. Александров был признан виновным в использовании программ, заведомо предназначенных для нейтрализации средств защиты компьютерной информации, совершенном из корыстной заинтересованности[213].

Суд установил, что субъективная сторона данного преступления характеризуется прямым умыслом. Интеллектуальный момент умысла выражался

---

[211] См.: Сверчков В.В. Указ. Соч. С. 332.

[212] Апелляционное определение СК по уголовным делам Московского городского суда от 1 марта 2021 г. по делу № 10-2228/2021 [Электронный ресурс]. – Доступ из СПС «Гарант».

[213] Приговор Кузьминского районного суда г. Москвы от 23 ноября 2020 г. по делу № 1-584/2020 [Электронный ресурс]. – Доступ из СПС «Гарант».

в осознании Александровым того, что используемые им программы предназначены именно для нейтрализации средств защиты и не имеют легального происхождения. В определении особо подчеркивается, что осужденный имел реальную возможность убедиться в отсутствии легальности устанавливаемых программ, что исключает неосознанность его действий. Волевой момент умысла проявился в желании Александрова использовать указанные программы, поскольку без их применения было невозможно достижение его конечной цели. Квалифицирующий признак ч. 2 ст. 273 УК РФ – корыстная заинтересованность – был подтвержден тем, что использование вредоносных программ служило средством получения материальной выгоды (денежного вознаграждения в размере 7000 рублей за установку контрафактного программного обеспечения).

Что касается таких факультативных признаков субъективной стороны, мотива и цели при совершении преступления, предусмотренного ст. 273 УК РФ, то в теории уголовного права их правовая природа и значение трактуются однозначно. Как отмечает М.М. Малыковцев, мотив и цель исследуемого преступления не входят в число обязательных признаков его основного состава[214]. Это означает, что установление конкретных побуждений и конечных задач виновного не является необходимым условием для квалификации его действий по данной статье.

Однако несмотря на их факультативный для квалификации характер, значение этих признаков для итоговой уголовно-правовой оценки деяния весьма существенно, поскольку они в обязательном порядке должны учитываться судом при индивидуализации наказания в рамках санкции статьи. Вместе с тем, как подчеркивает М.М. Малыковцев, существует ситуация, при которой мотив и цель могут приобрести роль обязательных признаков. Это происходит в случаях, когда создание, использование или распространение вредоносной программы является не самоцелью, а лишь способом достижения конечного преступного результата, т.е. когда виновный преследует цель совершить с ее помощью иное, более тяжкое преступление[215].

---

[214] См.: Малыковцев М.М. Указ. соч. С. 119.
[215] См.: там же.

Аналогичной позиции придерживается и М.А. Ефремова, указывая, что законодатель не предусмотрел мотив или цель в качестве обязательных элементов субъективной стороны, вследствие чего они не оказывают влияния на квалификацию, но подлежат учету при назначении наказания[216].

Пожалуй, необычный для ст. 273 УК РФ мотив прослеживается в деле Шестакова[217], что представляет интерес для анализа субъективной стороны состава преступления. Шестаков, являясь «сторонником либерального общественно-политического течения», совершил DDoS-атаку на официальный сайт политической партии в целях блокирования доступа пользователей к размещенной на нем информации. Судом установлен прямой умысел: виновный осознанно скопировал вредоносную программу и целенаправленно активировал ее в определенное время для нарушения работы ресурса. Ключевая особенность данного дела – мотив, носивший не корыстный (как в большинстве дел по ст. 273 УК РФ), а мировоззренческий, политический характер. Поскольку для основного состава ч. 1 ст. 273 УК РФ мотив не является конструктивным признаком, данное обстоятельство не повлияло на квалификацию, однако прокурор в апелляционном представлении безуспешно пытался обосновать им повышенную общественную опасность деяния, ссылаясь на интересы безопасности государства[218].

Думается, что совершение компьютерных преступлений, в том числе предполагающих использование вредоносных программ, по экстремистским мотивам стало объективной реальностью в настоящее время. Компьютерные атаки или вредоносная «техническая поддержка» хакерами могут и иногда фактически осуществляются по мотивам идеологической или политической ненависти, не исключены и мотивы ненависти национальной либо религиозной (когда объектами атак становятся официальные интернет-страницы тех или иных религиозных учреждений или организаций). Само по себе это является достаточным основанием

---

[216] См.: Ефремова М.А. Уголовно-правовая охрана информационной безопасности: дис. ... д-ра юрид. наук. М., 2017. С. 361.

[217] Приговор Бабушкинского районного суда г. Москвы от 13 октября 2015 г. по делу № 01-0656/2015 [Электронный ресурс]. – Доступ из СПС «Гарант».

[218] Апелляционное определение Московского городского суда от 27 ноября 2015 г. по делу № 10-16199/2015 [Электронный ресурс]. – Доступ из СПС «Гарант».

для того, чтобы обсуждать дальнейшее совершенствование системы квалифицирующих признаков ст. 273 УК РФ.

Однако изучение имеющейся в свободном доступе судебной практики не позволяет сделать вывод о том, что такие мотивы являются достаточно распространенными. До настоящего времени подобные действия в преобладающем большинстве (свыше 92%) продиктованы корыстными побуждениями. Кроме того, нельзя не указать и на то, что соответствующие мотивы совершения преступления с вредоносными компьютерными программами могут быть отражены и учтены судом в порядке применения п. «е» ч. 1 ст. 63 УК РФ.

Переходя к анализу субъективной стороны преступления, предусмотренного ст. 320 УК КР, представляется необходимым рассмотреть общие положения о вине в уголовном праве Кыргызстана.

Как справедливо отмечает Л.Ч. Сыдыкова, в теории уголовного права Кыргызской Республики понятие вины было разработано давно, однако свое четкое законодательное закрепление оно получило сравнительно недавно – в УК КР 2017 г. с последующим повторением в действующей редакции УК КР 2021 г.[219] Это принципиально важное нормативное установление содержится в ст. 29 УК КР, которое дает легальное определение вины как психического отношения лица к совершаемому им общественно опасному деянию (действию или бездействию), предусмотренному кодексом, и его противоправным последствиям.

Законодатель прямо закрепляет, что формами такого психического отношения могут быть умысел или неосторожность. Данная законодательная норма имеет фундаментальное значение для правильного понимания и толкования субъективной стороны любого преступления, включая и преступления в сфере компьютерной информации, поскольку она устанавливает единую методологическую основу для анализа вины, конкретизируя ее содержание.

Анализ субъективной стороны преступления, предусмотренного ст. 320 УК КР, позволяет выявить как сходства, так и существенные различия со

[219] См.: Сыдыкова Л. Ч. Уголовное право Кыргызской Республики. Общая часть. Преступление. Наказание: учебник. Бишкек : Издательский дом КРСУ, 2023. С. 214.

ст. 273 УК РФ. В доктрине уголовного права Кыргызстана по данному вопросу существуют определенные дискуссии. Так, по мнению З.К. Курманова и Р.А. Океновой, субъективная сторона данного деяния характеризуется исключительно прямым умыслом. Она указывает, что виновный осознает общественную опасность своих действий, а именно то, что он создает, использует или распространяет вредоносную программу или ее носитель, предвидя причинение вреда охраняемым законом интересам, и желает совершить эти действия[220].

При этом З.К. Курманова и Р.А. Окенова подчеркивают, что мотив и цель не являются обязательными признаками состава этого преступления и не влияют на его квалификацию[221].

Иной подход предлагает Т.М. Асаналиев и К.М. Осмоналиев, которые полагают, что субъективная сторона анализируемого деяния может характеризоваться как прямым, так и косвенным умыслом[222].

Следует отметить, что приведенные позиции ученых формировались в рамках доктринального осмысления предыдущих редакций уголовного закона Кыргызстана, действовавших до существенного реформирования, которое воплотилось в современной редакции 2021 г.

В настоящее время, с принятием новой редакции ст. 320 УК КР, дискуссия о субъективной стороне, возможно, требует нового осмысления с учетом измененных признаков объективной стороны, однако мнение указанных авторов остается важным историко-правовым аргументом, иллюстрирующим эволюцию подхода к этому составу преступления в кыргызской уголовно-правовой доктрине.

Учитывая действующую редакцию диспозиции ст. 320 УК КР, содержащую указания на «создание с целью использования либо распространения...», «заведомо предназначенные для осуществления…», «…умышленное использование и распространение таких программных продуктов, повлекших причинение

---

[220] См.: Курманов К.Ш. Указ. соч. С. 398.
[221] См.: там же.
[222] См.: Асаналиев Т.А., Осмоналиев К.М. Комментарий к Уголовному кодексу (постатейный). Преступления и наказания в Кыргызской Республике. Бишкек, 2004. С. 537.

значительного ущерба или иного значительного вреда…», представляется обоснованной поддержка именно первого подхода.

Отличием субъективной стороны преступления, предусмотренного ст. 320 УК КР, от ст. 273 УК РФ является прямое указание в диспозиции на специальную цель. Формулировка в ст. 320 УК КР «Создание с целью распространения или использования…» свидетельствует о том, что цель в данном составе является конструктивным, обязательным признаком субъективной стороны, что коренным образом меняет ее юридическое значение по сравнению с факультативной целью в российском уголовном праве. Таким образом, субъективная сторона преступления по ст. 320 УК КР характеризуется умышленной формой вины (прямой умысел) и наличием специальной цели – распространения или использования создаваемой вредоносной программы.

Таким образом, если в российском праве такой признак, как цель, является факультативным признаком субъективной стороны, то в кыргызском уголовном законе она становится обязательным признаком состава, по крайней мере, в части, касающейся создания вредоносных программ, что существенным образом отличает психическое отношение виновного, подлежащее доказыванию по данной статье. Выявленное различие имеет принципиальное значение для правоприменения. Указание в ст. 320 УК КР на специальную цель, с одной стороны, усиливает гарантии для невиновных лиц (например, исследователей, создающих вредоносные программы в научных целях), поскольку отсутствие цели исключает состав преступления. С другой стороны, доказывание субъективной цели всегда сложнее, чем доказывание объективного факта создания, что может создавать трудности для обвинения и порождать риски необоснованного оправдания при явно противоправном характере действий. Каждый из подходов имеет свои достоинства и недостатки, и их выбор зависит от приоритетов уголовной политики государства

Не менее важным вопросом является практический алгоритм установления субъективной стороны преступлений, предусмотренных ст. 273 УК РФ и ст. 320 УК КР. В соответствии с правовой позицией, изложенной в п. 3 постановления Пленума Верховного Суда РФ № 1 «О судебной практике по делам

об убийстве (ст. 105 УК РФ)»[223] квалификация по признакам субъективной стороны всегда дается через интерпретацию правоприменителем объективных фактов. Иной способ установления вины, умысла, цели и мотива в уголовном праве отсутствует. Данный алгоритм универсален и применим к любым составам преступлений, включая деяния, связанные с вредоносными компьютерными программами.

В случае со ст. 273 УК РФ и ст. 320 УК КР, характер приобретения программы, наличие или отсутствие легального разрешения на ее использование, специальные знания лица, профессиональный опыт или обстоятельства ее применения через перечисленные объективные обстоятельства возможно установить заведомость.

Однако, цель использования или распространения, предусмотренная ст. 320 УК КР через анализ действий лица, а именно было ли распространение, использовалась ли программа в отношении чужих информационных систем, предпринимал ли виновный меры к сокрытию своих действий.

Отсутствие легитимной цели, допустим при создании программы с вредоносными свойствами указывает на прямой умысел, а также через последствия, которые объективно наступили и виновный не мог предвидеть.

В большинстве случаев, субъективная сторона познается правоприменителем через анализ объективных фактов, которые в своей совокупности позволяют сделать вывод о том, что виновный осознавал вредоносных характер и желал действовать определенным образом, а не путем опроса лица о его намерениях. Настоящий подход, выработан на протяжении многолетней судебной практики по «классическим» составам и также применим к компьютерным преступлениям, в части доказывания субъективной стороны.

Субъект преступления является неотъемлемой частью любого состава, поскольку его установление напрямую связано с основанием уголовной

---

[223] Постановление Пленума Верховного Суда РФ от 27 января 1999 г. № 1 «О судебной практике по делам об убийстве (ст. 105 УК РФ)» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_21893/ (дата обращения: 30.05.2026).

ответственности (ст. 8 УК РФ) и принципом юридической определенности (ст. 3 УК КР). Согласно ч. 1 ст. 24 УК КР, субъектом преступления является физическое вменяемое лицо, совершившее преступление в возрасте, с которого в соответствии с кодексом наступает уголовная ответственность.

В доктрине уголовного права Кыргызской Республики под субъектом преступления понимается лицо, совершившее противоправное деяние и способное в соответствии с законом нести за него уголовную ответственность[224]. Таким образом, общий субъект характеризуется тремя признаками: физическое лицо, вменяемость и достижение установленного законом возраста.

Аналогичный подход наблюдается в российском законодательстве. Так по мнению К. Н. Евдокимова, исходя из смысла ст. 19 УК РФ, основными признаками субъекта компьютерных преступлений также являются принадлежность к физическим лицам, вменяемость и достижение возраста уголовной ответственности[225].

Для большинства составов, включая ст. 273 УК РФ и ст. 320 УК КР, эти признаки являются универсальными, поэтому в доктрине уголовного права обосновано выделяют понятие общего субъекта, который наделен общими базовыми признаками, и специального субъекта, помимо наличия базовых критериев обладает дополнительными характеристиками, указанными в диспозиции конкретной нормы.

Важнейшим аспектом является то, что если преступление совершено лицом, не отвечающим установленным законом критериям, например невменяемым или не достигшим возраста уголовной ответственности, то вопрос о привлечении его к уголовной ответственности не возникает. Кроме того, принципиальное значение имеет законодательное закрепление в ч. 3 ст. 24 УК КР положения о том, что субъектом преступления может быть только физическое лицо – человек, что автоматически исключает уголовную ответственность юридических лиц.

---

[224] См.: Сыдыкова Л.Ч. Уголовное право Кыргызской Республики. Общая часть. Преступление. Наказание: учебник. Бишкек : Издательский дом КРСУ, 2023. С. 253.

[225] См.: Евдокимов К.Н. Противодействие компьютерной преступности: теория, законодательство, практика: дис. ... д-ра юрид. наук. М., 2021. С. 344–345.

Фундаментальные положения могут быть применимы в равной степени при характеристике субъекта как по ст. 320 УК КР, так и по ст. 273 УК РФ. В обоих случаях речь идет об общем субъекте – физическом вменяемом лице, достигшем 16-летнего возраста, что вытекает из системного анализа уголовных кодексов обеих стран и природы данных преступлений, не предполагающих наличия специальных признаков у виновного.

Однако при переходе к квалифицированным составам проявляются ключевые различия. В ч. 2 ст. 273 УК РФ в числе квалифицирующих признаков прямо указано совершение преступления «лицом с использованием своего служебного положения». Это наделяет субъекта в таком составе специальными признаками, превращая его из общего в специального субъекта преступления.

В российской правоприменительной практике квалификация преступных действий с вредоносными компьютерными программами лицом с использованием своего служебного положения имеет место в случаях, когда соответствующие деяния совершаются сотрудником в силу его должностных обязанностей и полномочий, предоставляющих ему особый доступ к компьютерной информации или управленческие функции[226].

В российской правоприменительной практике наиболее ярким примером осуждения лиц за использование вредоносных компьютерных программ лицами с использованием своего служебного положения стала целая серия обвинительных приговоров (преимущественно в южных регионах России) в отношении служащих автозаправочных станций: «…являясь инженером сектора информационных технологий, автоматизации и метрологии ООО “РН-Волгоград”, используя свои профессиональные знания и служебное положение…Указанная программа позволяла модифицировать компьютерную информацию, а именно, изменять данные о весе отпускаемого топлива в товарно-транспортных накладных, что приводило к недоливу клиентам... действуя из корыстной заинтересованности и в силу своих служебных обязанностей по обслуживанию программного обеспечения,

---

[226] См.: Евдокимов К.Н. Противодействие компьютерной преступности: теория, законодательство, практика: дис. ... д-ра юрид. наук. М., 2021. С. 538–539.

систематически обеспечивал работоспособность вредоносной программы, устранял сбои в ее работе и получал за это денежное вознаграждение от организаторов...». Суды квалифицировали такие действия именно по ч. 2 ст. 273 УК РФ как использование компьютерной программы, заведомо предназначенной для несанкционированной модификации компьютерной информации, лицом с использованием своего служебного положения, из корыстной заинтересованности[227].

В ст. 320 УК КР аналогичный признак отсутствует. В кыргызском уголовном законе квалифицирующими признаками являются совершение деяния группой лиц по предварительному сговору, причинение по неосторожности крупного ущерба, а также направленность деяния на критическую информационную инфраструктуру, но не использование своего служебного положения. Представляется, что российский опыт криминализации использования служебного положения мог бы быть полезен для Кыргызстана при совершенствовании ст. 320 УК КР.

Проведенное нами социологическое исследование показало, что большинство респондентов – 59,7% – поддерживают необходимость включения в ст. 320 УК КР квалифицирующего признака *«совершение деяния лицом с использованием своего служебного положения»*. Еще 22,6% опрошенных в целом согласны с данным предложением, хотя и допускают возникновение определенных сложностей в правоприменительной практике при разграничении законных полномочий сотрудника и его преступных действий. Таким образом, совокупная доля респондентов, положительно оценивающих данную законодательную новеллу, превышает 82%, что свидетельствует о явном запросе на ужесточение ответственности для так называемых инсайдеров. При этом лишь незначительная часть респондентов анкетирования (по 6,5%) посчитала данную меру избыточной ввиду достаточности существующих норм о должностных преступлениях либо

[227] Приговор Дзержинского районного суда города Волгограда Волгоградской области от 15 ноября 2018 г. по делу № 1-357/2018 [Электронный ресурс]. – Доступ из СПС «Гарант».

вовсе не усматривающей зависимости степени общественной опасности действий с вредоносной программой от статуса распространителя[228].

Вместе с тем это обусловлено целым рядом причин. Прежде всего важно указать на то, что использование лицом своих управленческих полномочий в организации всегда существенным образом влияет на степень общественной опасности конкретного посягательства. С другой стороны, такие действия априорно причиняют вред не только непосредственному объекту (в нашем случае – отношениям в сфере информационной безопасности), но и интересам службы. Общепринятым и не требующим дополнительной аргументации является и представление о том, что специальный статус субъекта, как правило, осложняет выявление и доказывание по подобного рода делам.

В завершение следует еще раз сослаться на подход Республики Молдова, где, как ранее было отмечено в § 3 гл. 1, уголовная ответственность за аналогичные деяния наступает с 14 лет (ч. 2 ст. 21 УК Молдовы), а также предусмотрена ответственность юридических лиц. Хотя прямое заимствование данных норм в Кыргызскую Республику в настоящий момент не предлагается, сам факт наличия таких альтернативных подходов в рамках СНГ подтверждает, что универсальной модели субъекта не существует и выбор возраста ответственности является результатом национальной уголовной политики.

[228] Результаты опроса в Приложении № 1 к диссертации.

ГЛАВА 3. ПЕРСПЕКТИВНЫЕ НАПРАВЛЕНИЯ СОВЕРШЕНСТВОВАНИЯ ЗАКОНОДАТЕЛЬСТВА И ПРОБЛЕМЫ КВАЛИФИКАЦИИ СОЗДАНИЯ, ИСПОЛЬЗОВАНИЯ И РАСПРОСТРАНЕНИЯ ВРЕДОНОСНЫХ КОМПЬЮТЕРНЫХ ПРОГРАММ

§ 1. Особенности и проблемы квалификации создания, использования и распространения вредоносных компьютерных программ

Выявление и комплексный анализ особенностей, проблем деяний, предусмотренных ст. 273 УК РФ и ст. 320 УК КР является целью настоящего параграфа. Достигнуть поставленной цели, возможно, с помощью исследования спорных вопросов правоприминительной практики. Безусловно, сопоставление позволит не только углубиться в понимании национальных механизмов противодействия киберпреступности, но и выявить потенциальные направления, которые помогут совершенствовать законодательство в целях повышения эффективности в борьбе с киберпреступностью.

Согласно точке зрения К.Н. Евдокимова, одной из ключевых мер противодействия компьютерной преступности является уголовное преследование виновных лиц. Однако для его эффективности система правосудия должна постоянно совершенствоваться, основываясь на анализе изменяющихся информационных отношений и глубоком понимании технологических средств, которые могут быть использованы в преступных целях[229].

Одним из наиболее дискуссионных вопросов в рамках применения уголовного закона о компьютерных преступлениях остается определение понятия «вредоносная программа»[230]. В теории уголовного права и в правоприменительной практике неизбежно возникают неоднозначные ситуация из-за отсутствия четкого определения данного термина в законодательстве. В связи с этим, судебные и

---

[229] См.: Евдокимов К.Н. Противодействие компьютерной преступности: теория, законодательство, практика: дис. ... д-ра юрид. наук. М., 2021. С. 376.

[230] См.: Евдокимов К.Н. Принципы противодействия технотронной преступности: онтологические и гносеологические аспекты // Российская юстиция. 2020. № 3. С. 56–58.

следственные органы вынуждены опираться исключительно на результаты экспертиз. Однако, эксперты могут использовать разную методологию анализа, что приводит к вариативности выводов касательно функционального предназначения того или иного кода.

Определенную ориентирующую роль играет разъяснение, данное в постановлении Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37, согласно которому по ст. 273 УК РФ подлежат наказанию действия лишь с теми программами, которые заведомо предназначены для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств ее защиты[231]. Даже с учетом данного разъяснения, остается пространство для дискуссии между экспертами, так как ключевым фактом становится установления предназначения программы, которое на практике сводится к анализу функциональных возможностей и алгоритмов. Вероятна следующая ситуация, например, где один и тот же программный код со способностью к самокопированию, одним экспертом может быть расценен как вредоносный троян, а другой посчитает инструментом для легитимного администрирования сетей.

Думается, что аналогичная проблема свойственна и правоприменительной практике Кыргызской Республики, где норма также оперирует понятием «вредоносный программный продукт». Однако, в ходе исследования, выяснилось, что получить непосредственный доступ к материалам судебно-следственной практики Кыргызстана по делам о компьютерных преступлениях в целом представляет серьезную проблему.

В ходе работы над исследованием были подготовлены и направлены запросы в Генеральную прокуратуру Кыргызской Республики и Национальный статистический комитет Кыргызской Республики. Согласно полученным ответам

---

[231] 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». URL: https://www.consultant.ru/document/cons_doc_LAW_434573/ . (дата обращения: 20.11.2025).

Национальный статистический комитет Кыргызской Республики сообщил об отсутствии запрашиваемых сведений. В свою очередь, Генеральная прокуратура Кыргызской Республики предоставила необходимые сведения. Согласно предоставленным сведениям о статистических данных по количеству совершаемых преступлений в сфере компьютерной информации за 2021–2025 гг., в частности по ст. 320 УК КР, зафиксированы следующие показатели: за 2021 г. – 1; за 2022–2024 гг. – 0; за 2025 г. – 7[232].

В отсутствие систематизированной официальной статистики эмпирическую базу исследования составили данные из открытых источников, которые, по существу, замещают анализ правоприменения по Кыргызской Республике. Так, 19 октября 2023 г. сайт Государственной налоговой службы КР подвергся хакерской атаке, предположительно силами вьетнамских хакеров, что привело к временному ограничению доступа к порталу. Данный инцидент иллюстрирует уязвимость государственных информационных ресурсов, однако уголовно-правовая квалификация подобных деяний по ст. 320 УК КР остается неизвестной широкой аудитории[233].

Более показательным является исследование компании «Доктор Веб», опубликовавшей результаты масштабного анализа целевых атак на государственные учреждения Казахстана и Кыргызской Республики. Поводом послужили обращения представителей госучреждений Кыргызской Республики, подозревавших наличие вредоносных программ в своих сетях. Аналитикам удалось выявить два типа троянов: массовые, распространенные на большинстве компьютеров сети, и специализированные, установленные на серверы. Особый интерес представляет неизвестное ранее семейство троянов XPath, обладающих руткитом – механизмом для сокрытия сетевой активности и следов присутствия в системе. Другой троян – Mirage – использовал файлы, позволившие зафиксировать

---

[232] Приложение № 2 к диссертации.

[233] Сайт Налоговой службы Кыргызстана подвергся хакерской атаке. URL: https://ru.sputnik.kg/20231019/sayt-nalogovoy-sluzhby-kyrgyzstana-podvergsya-khakerskoy-atake-1079673967.html (дата обращения: 11.04.2026).

команды злоумышленников и полученные данные[234]. Этот кейс важен для понимания того, как технически сложные вредоносные программы (подпадающие под признаки ст. 320 УК КР) применяются в реальных атаках, однако уголовные дела по данным фактам, вероятно, не дошли до суда или находятся на стадии следствия, материалы которого недоступны.

Статистические данные, хотя и опосредованные, предоставляют аналитику «Лаборатории Касперского»: каждый 30-й компьютер в Кыргызстане с начала 2025 г. был атакован вредоносным программным обеспечением. Как отмечает в интервью «Российской газете» экс-министр цифрового развития Кыргызской Республикой Нурия Кутнаева, официальной статистики по Кыргызстану в открытом доступе нет, и эти данные учитывают лишь точки с лицензионными антивирусными пакетами. Эксперт также обращает внимание на рост фишинговых атак, когда мошенники под видом доверенных организаций, включая государственные органы, вынуждают пользователей перейти по ссылке, что ведет к заражению устройства без каких-либо дополнительных действий. Характерно, что такие атаки используют человеческие слабости – страх, любопытство или жажду легкой наживы[235]. Данный тезис важен для уголовно-правовой оценки: в отличие от классического «вредоносного программного обеспечения», фишинговые ссылки могут формально не являться программами, но нередко ведут к установке таковых, что порождает проблемы квалификации как по ст. 273 УК РФ, так и по ст. 320 УК КР.

Особого внимания заслуживает инцидент от 22 мая 2024 г., когда хакерская группа Team Insane Pakistan опубликовала персональные данные более 600 тысяч граждан Кыргызстана. Анализ показал, что данные оказались идентичны утечке 2020 г. из базы налогоплательщиков (879 тыс. записей), когда сайт www.salyk.kg был взломан через SQL-инъекцию. При этом сама группа обычно занимается

---

[234]См.: По следу хакеров. URL: https://www.kommersant.ru/doc/4432198?ysclid=mnd9pny0hu401328144 (дата обращения: 11.04.2026).

[235] См.: В Кыргызстане каждый тридцатый компьютер атакуют вредоносные программы. URL: https://rg.ru/2025/06/04/v-kyrgyzstane-kazhdyj-tridcatyj-kompiuter-atakuiut-vredonosnye-programmy.html?ysclid=mnd9ulpmbs703845578&utm_referrer=https%3A%2F%2Fyandex.ru%2F (дата обращения: 13.04.2026).

DDoS-атаками, а не кражей данных[236]. Данный случай важен в контексте ст. 320 УК КР по двум причинам: во-первых, сам взлом сайта и извлечение базы данных (в 2019-2020 гг.) является классическим примером неправомерного доступа с использованием вредоносного кода (SQL-инъекция – это, по сути, вредоносная команда); во-вторых, переопубликование тех же данных спустя годы показывает, что вредоносные программы и их последствия имеют длительный латентный период, а ответственность по ст. 320 УК КР (как и по ст. 273 УК РФ) должна охватывать не только создание, но и распространение и использование.

Важным контекстуальным дополнением является обсуждение перспектив присоединения Кыргызской Республики к Будапештской конвенции о киберпреступности от 2001 г. Как отмечается в аналитической статье, в 2024 г. принят Закон КР «О кибербезопасности Кыргызской Республики», однако количество зарегистрированных преступлений с использованием ИКТ выросло на 37% (данные МВД КР за 2024 г.). Эксперты полагают, что реальные цифры выше из-за низкой раскрываемости и нехватки квалифицированных кадров. Присоединение к Будапештской конвенции от 2001 г., по мнению специалистов, позволило бы Кыргызстану получить доступ к международным каналам оперативного взаимодействия (сеть 24/7) и обязать глобальные платформы (Meta, Google, TikTok) сотрудничать по запросам о сохранении и выдаче данных[237]. Однако с точки зрения уголовного права важно, что Будапештская конвенция от 2001 г. предусматривает унификацию законодательства в сфере киберпреступлений, включая гармонизацию ст. 320 УК КР. На сегодняшний день отсутствие единого подхода к определению «вредоносной программы» и разобщенность правоприменительной практики Кыргызстана, о чем свидетельствует отсутствие доступа к судебным актам, существенно затрудняют как национальное расследование, так и международное сотрудничество.

---

[236] См.: Хакеры «слили» в Сеть персональные данные 630 тысяч кыргызстанцев. URL: https://economist.kg/novosti/2024/06/05/khakiery-slili-v-siet-piersonalnyie-dannyie-630-tysiach-kyrghyzstantsiev/?ysclid=mnd9xgnxq847623602 (дата обращения: 14.04.2026).

[237] См.: Кыргызстан и Будапештская конвенция: цифровая безопасность как вызов времени. URL: https://mnenie.akipress.org/unews/un_post:44659/ (дата обращения: 14.04.2026).

Таким образом, проведенный анализ новостных и экспертных источников позволяет сделать следующие выводы. Во-первых, фактическая распространенность вредоносного программного обеспечения в Кыргызстане (каждый 30-й компьютер атакован) и наличие реальных инцидентов с госучреждениями свидетельствуют о высокой общественной опасности деяний, предусмотренных ст. 320 УК КР. Во-вторых, отсутствие открытой судебно-следственной практики по ст. 320 УК КР создает серьезные препятствия для сравнительно-правового исследования и, вероятно, для единообразного применения закона. В-третьих, многие кибератаки, такие как фишинг, SQL-инъекции, трояны с руткитам технически подпадают под признаки ст. 320 УК КР, однако их правовая оценка требует разграничения со смежными составами, например, неправомерный доступ – ст. 319 УК КР или мошенничество – ст. 209 УК КР. В условиях ограниченного доступа к правоприменительным актам Кыргызской Республики, новостные материалы следует рассматривать в качестве эмпирического замещения.

Анализ судебной практики по делам, связанным со ст. 273 УК РФ, и, в частности, подробное рассмотрение дела в отношении Кочкина[238] демонстрирует, как суды на практике решают сложную задачу квалификации программного обеспечения как вредоносного в условиях законодательной неопределенности данного понятия.

Можно отметить, что на совокупность обстоятельств, которые интерпретируются через призму внутренних регламентов и экспертных заключений, ложится ключевая нагрузка в процессе доказывания заведомой предназначенности программы.

В деле Кочкина суд первой инстанции, а затем и апелляция[239] сформировали позицию, опираясь на комплекс доказательств, центральное место в котором заняли не столько свойства самого кода, сколько контекст его создания и

---

[238] Приговор Железнодорожного районного суда г. Новосибирска Новосибирской области от 23 мая 2025 г. по делу № 1-24/2025 [Электронный ресурс]. – Доступ из СПС «Гарант».

[239] Апелляционное постановление Новосибирского областного суда от 5 сентября 2025 г. по делу № 22-3384/2025 [Электронный ресурс]. – Доступ из СПС «Гарант».

использования. Судом было установлено, что подсудимый, являясь администратором системы ФИС ГИБДД-М и будучи должностным лицом, знал о строгих запретах на внесение любых изменений в работу сервиса, о существовании специального антикоррупционного механизма случайной выдачи номерных знаков и о том, что функция возврата знака была целенаправленно отключена федеральным администратором. Именно этот служебный контекст и знание внутренних правил стали для суда основой для вывода о «заведомости», т.е. о понимании Кочкиным противоправного характера своих действий с момента создания программы.

Вредоносность программы оценивалась судом не через призму ее внутренней архитектуры (например, наличие вирусного кода), а через ее функциональный результат – несанкционированное изменение интерфейса и обход установленного организационного порядка. Заключения специалистов при этом сыграли решающую роль, дав суду техническое обоснование для терминов «модификация» и «нейтрализация средств защиты». Они пояснили, что модификация – это любое изменение кода, в том числе реактивация скрытого элемента, а под средствами защиты понимаются не только технические, но и организационно-правовые меры, такие как приказ об отключении функции. Таким образом, судебная практика в этом деле фактически расширительно истолковала понятие «нейтрализации средств защиты», включив в него преодоление административных запретов и восстановление функционала, выключенного уполномоченным лицом.

В последующем, защита с помощью альтернативного заключения эксперта пыталась оспорить выводы обвинения, но суд отклонил его из-за процессуальных недостатков, то есть исследование было проведено без соблюдения порядка, установленного УПК, а также без предупреждения специалиста об уголовной ответственности. Соответственно, судебное решение о вредоносности программы, в какой-то степени зависит от того, чье заключение будет признано судом допустимым, обвинения или защиты. Решение по делу Кочкина только подтверждает, что в отсутствие четких законодательных дефиниций суды вынуждены определять качество вредоносности программы ситуативно.

Другим не менее актуальным и спорным вопросом является возможность признания вредоносным программным обеспечением VPN-сервисов либо приложений со встроенным VPN-функционалом[240]. Проблема порождена технической двойственностью таких сервисов: с одной стороны, они могут использоваться для законного обхода региональных блокировок и защиты персональных данных, с другой – их целенаправленное применение способно нейтрализовать средства идентификации пользователя, установленные провайдером или государственными органами в рамках правового режима. Российская судебно-следственная практика демонстрирует пример расширительного толкования признака «нейтрализация средств защиты компьютерной информации» применительно к VPN-технологиям.

Показательным, но спорным примером является приговор Октябрьского районного суда г. Томска от 21 октября 2022 г. в отношении Белоуса по ч. 1 ст. 273 УК РФ. Суть предъявленного обвинения состояла в том, что Белоус, находясь по месту своего проживания в квартире и используя принадлежащий ему персональный компьютер с доступом к сети «Интернет», осуществил поиск вредоносной компьютерной программы “Vipole”, выражающейся в невозможности однозначной идентификации пользователя сети «Интернет» и его сетевой активности, в том числе провайдером, предоставляющим доступ к сети «Интернет» и заведомо для него предназначенной для нейтрализации средств защиты компьютерной информации провайдеров, направленных на однозначную идентификацию пользователя в сети «Интернет». Тем самым суд фактически признал VPN-подобный сервис (программу, маскирующую сетевой трафик) вредоносной компьютерной программой по признаку ее функционального назначения[241]. Данный подход является спорным, поскольку технически VPN-шифрование не «нейтрализует» средства защиты провайдера в смысле их взлома или повреждения, а лишь создает альтернативный зашифрованный канал,

---

[240] См.: Русскевич Е.А. Компьютерные преступления: квалификационные алгоритмы и тренды: учеб. пособие. М., 2025. С. 44.

[241] Приговор Октябрьского районного суда г. Томска от 21 октября 2022 г. по делу 1-981/2022 [Электронный ресурс]. – Доступ из СПС «Гарант».

непрозрачный для систем глубокого анализа пакетов (DPI). Тем не менее с точки зрения телеологического толкования ст. 273 УК РФ законодательная цель – обеспечение возможности правоохранительного и регуляторного контроля за сетевым трафиком – может быть достигнута лишь при условии запрета программ, целенаправленно скрывающих идентификационные признаки пользователя.

В противоположность этому, безусловно обоснованным является приговор Центрального районного суда г. Читы от 3 июня 2025 г. в отношении братьев Божка М.С. и Божка А.С. Суд установил, что осужденные распространяли в сети «Интернет» вредоносное программное обеспечение, замаскированное под приложение VPN-сервиса. Пользователи, не подозревая о преступных намерениях, скачивали и устанавливали программу, которая в действительности представляла собой троянское приложение семейства «стилеров», предназначенное для несанкционированного копирования пользовательских данных (логинов, паролей, информации из мессенджеров и криптокошельков), их модификации и нейтрализации средств защиты компьютерной информации. В данном случае суд обоснованно квалифицировал действия осужденных по ч. 2 ст. 273 УК РФ, поскольку вредоносность программы определялась ее действительным функционалом, подтвержденным заключением экспертизы «Лаборатории Касперского», а не внешней оболочкой[242]. VPN-маскировка в этом деле выступала лишь как способ распространения вредоносного программного обеспечения, но не как основание для признания легитимных VPN-сервисов «вредоносными».

Однако единичный случай, связанный с осуждением Белоуса за использование программы “Vipole”, не может и не должен рассматриваться в качестве достаточного основания для признания VPN-сервисов вредоносными программами в широком смысле. На практике суды не признают «честный» VPN-сервис, т.е. программу, легитимно обеспечивающую шифрование трафика и изменение IP-адреса, вредоносной компьютерной программой исключительно в силу наличия у нее функции анонимизации.

---

[242] Приговор Центрального районного суда г. Читы от 3 июня 2025 г. по делу № 1-371/2025 [Электронный ресурс]. – Доступ из СПС «Гарант».

Данная позиция находит свое подтверждение в анализе приговоров Индустриального районного суда г. Барнаула Алтайского края от 6 октября 2025 г. в отношении Яцковского (ч. 2 ст. 273 УК РФ), Одинцовского городского суда Московской области от 31 октября 2025 г. в отношении Галеева (ч. 3 ст. 273 УК РФ, ч. 4 ст. 272 УК РФ, ч. 3 ст. 30 УК РФ, ч. 4 ст. 159^6 УК РФ) и Киселевского городского суда Кемеровской области от 24 ноября 2025 г. в отношении Трунова (ч. 1 ст. 273 УК РФ). В указанных делах, несмотря на то, что подсудимые использовали различные средства анонимизации и сокрытия своего местонахождения в сети «Интернет», суды ни в одном из случаев не квалифицировали сам VPN-клиент как вредоносную программу по ст. 273 УК РФ. В частности, в деле Трунова подсудимый использовал «OpenVPN» для маскировки реального IP-адреса при проведении компьютерных атак, однако уголовная ответственность наступила за использование программ “SQLMap” и “Acunetix”, предназначенных для несанкционированного уничтожения, блокирования и модификации компьютерной информации[243]. Аналогичным образом в деле Галеева соучастники арендовали серверы и настраивали на них VPN-соединения для сокрытия сетевой активности, но суд квалифицировал как вредоносное программное обеспечение скрипты на языке Python, осуществлявшие подбор ПИН-кодов и обход CAPTCHA, а также сам факт неправомерного доступа и покушения на мошенничество[244]. Что касается дела Яцковского, то осужденный использовал вредоносные программы по названиями Masscan, RouterScan, Metasploit Framework для сканирования IP-адресов в России, обнаружения уязвимостей и несанкционированного удаленного доступа к компьютерной информации организаций. В данном случае используемый OpenVPN, VDS-серверы применялся им не как вредоносное средство, а как технический инструмент сокрытия следов – для маскировки реального IP-адреса при проведении атак[245]. Судебная практика

[243] Приговор Киселевского городского суда Кемеровской области от 24 ноября 2025 г. по делу № 1-312/2025 [Электронный ресурс]. – Доступ из СПС «Гарант».
[244] Приговор Одинцовского городского суда Московской области от 31 октября 2025 г. по делу № 1-1023/2025 [Электронный ресурс]. – Доступ из СПС «Гарант».
[245] Приговор Индустриального райнного суда г. Барнаула Алтайского края от 6 октября 2025 г. по делу № 1-408/2025 [Электронный ресурс]. – Доступ из СПС «Гарант».

показывает следующее, что по смыслу ст. 273 УК РФ, VPN- сервис, который легитимно обеспечивает шифрование не является вредоносной программой. Необходимо установить деструктивный потенциал у программы, чтобы признать ее вредоносной, которое должно подтверждаться заключением компьютерно-технической экспертизы. Сама по себе функция анонимизации, при отсутствии иных деструктивных свойств, не образует состава преступления, предусмотренного ст. 273 УК РФ.

В контексте настоящего исследования особый интерес представляет квалификация деяний, связанных с разработкой и сбытом так называемого игрового вспомогательного программного обеспечения – читов и ботов для многопользовательских онлайн-игр. Отнесение указанных программ к категории вредоносных обусловлено не столько их способностью к саморепликации или явному уничтожению данных, сколько их функциональным назначением – несанкционированной модификацией компьютерной информации, защищенной средствами «античита», и вмешательством в штатный алгоритм работы серверной и клиентской частей программного комплекса. Необходимо согласиться с тем, что вредоносность в контексте игровых программ проявляется в изменении логики работы защищенного кода, что создает необоснованные преимущества для пользователя и дестабилизирует экономическую модель игровой экосистемы, нанося репутационный и материальный ущерб правообладателю[246].

Яркой иллюстрацией является дело в отношении Кирсанова, рассмотренное Верх-Исетским районным судом г. Екатеринбурга. В ходе расследования было установлено, что Кирсанов организовал разработку и сбыт через специализированные интернет-ресурсы (Cyber Tank и Cyber Ship) программного обеспечения, предназначенного для автоматизированного управления игровым процессом (боты) в многопользовательских онлайн-играх “World of Tanks” и “World of Warships”. Экспертным заключением было подтверждено, что указанные программы приводили к модификации компьютерной информации игрового

[246] См.: Русскевич Е.А. Компьютерные преступления: квалификационные алгоритмы и тренды: учеб. пособие. С. 48–49.

клиента, нейтрализуя встроенные механизмы защиты и позволяя пользователям получать нечестное преимущество в виде накопления внутриигровой валюты и опыта без непосредственного участия человека в соревновательном процессе. Суд квалифицировал действия подсудимого по ч. 2 ст. 273 УК РФ[247].

Примечательно, что объем общественно опасных последствий в данном деле был оценен потерпевшей стороной – компанией “Wargaming” – в размере 670 млн рублей, что свидетельствует о высокой латентной опасности данного сегмента компьютерной преступности и необходимости его уголовно-правовой оценки не только в России, но и в иных юрисдикциях постсоветского пространства[248].

Данный кейс для Кыргызстана является наглядным примером того, что конструкция ст. 320 УК КР, оперирующая понятиями несанкционированной модификации информации и заведомого предназначения программы для несанкционированного воздействия, обладает достаточной гибкостью для инкриминирования аналогичных деяний, совершаемых на территории республики или в трансграничном цифровом пространстве.

Кроме того, эволюция киберугроз в сфере гейминга не стоит на месте, так, в 2025 г. на примере выявленного вредоносного программного обеспечения «Webrat». В отличие от классических читов и ботов, которые непосредственно направлены на изменение игровых алгоритмов и образуют состав преступления исключительно по ст. 273 УК РФ, программный комплекс «Webrat», маскирующийся под чит-коды для игр “Rust”, “Counter Strike” и “Roblox”, демонстрирует переход количественных изменений в качественные. Webrat, помимо вмешательства в игровой процесс, содержит функционал кражи аутентификационных данных учетных записей “Steam”, “Discord” и “Telegram”,

---

[247] Приговор Верх-Исетский районного суда г. Екатеринбурга от 6 июля 2022 г. по делу № 1-382/2022 [Электронный ресурс]. – Доступ из СПС «Гарант».

[248] В России вынесли первый приговор за продажу читов для World of Tanks. URL: https://www.rbc.ru/rbcfreenews/62c5cbae9a794702dc6c2b6f (дата обращения: 15.04.2026).

скрытого наблюдения через веб-камеру и загрузки стороннего вредоносного программного обеспечения (майнеров, блокировщиков)[249].

В контексте исследования проблемы уголовно-правовой квалификации деяний в сфере компьютерной информации существенные сложности возникают при разграничении составов преступлений, предусмотренных ст. 272 УК РФ «Неправомерный доступ к компьютерной информации» и ст. 273 УК РФ.

Данная проблема носит не только теоретический, но и выраженный практический характер, что подтверждается материалами судебной практики. Несмотря на наличие разъяснений, содержащихся в постановлении Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37, где подчеркивается, что суть неправомерного доступа заключается в получении или использовании информации без согласия ее обладателя либо с нарушением установленного порядка, на практике сохраняется высокая вероятность конкуренции указанных составов[250].

В практике зачастую возникает сложность, когда способы использования вредоносных программ, формально подпадают под признаки ст. 272 УК РФ. Получается, что одно противоправное деяние может одновременно содержать объективные признаки обоих преступлений, в связи с этим перед правоприменителем возникает сложная задача в выборе окончательной квалификации.

Исходя из судебной практики, видно, что суды не всегда следуют единообразному подходу, поэтому это влечет за собой риски нарушения принципов справедливости и законности. Следовательно, возникает проблема

---

[249] Эксперты выявили вредоносное ПО Webrat для кражи данных геймеров и чит-кодов к играм. URL: https://www.forbes.ru/tekhnologii/537866-eksperty-vyavili-vredonosnoe-po-webrat-dla-krazi-dannyh-gejmerov-i-cit-kodov-k-igram (дата обращения: 15.04.2026).

[250] 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 «Консультантлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_434573/ . (дата обращения: 15.04.2026).

разграничения, которая требует дальнейшего осмысления в целях выработки более четких и практических критериев.

В качестве примера можно привести постановление Седьмого кассационного суда общей юрисдикции от 9 октября 2024 г.[251], где изначально вмененные осужденному действия по ч. 3 ст. 272 УК РФ были переквалифицированы судом апелляционной инстанции на подстрекательство к использованию вредоносной программы по ч. 4 ст. 33, ч. 2 ст. 273 УК РФ. При этом суд кассационной инстанции поддержал данный подход, указав, что действия осужденного были направлены именно на склонение другого лица к использованию специальной программы-патчера для нейтрализации средств защиты лицензионного программного обеспечения, что охватывается ст. 273 УК РФ, а не ст. 272 УК РФ.

Похожая ситуация разграничения наблюдается и в более ранней практике, например постановление Оренбургского областного суда от 17 ноября 2016 г.[252], где суд исключил из осуждения вмененную ч. 2 ст. 272 УК РФ, признав ее излишней, поскольку действия осужденного по копированию контрафактного программного обеспечения и последующему использованию вредоносной программы для обхода защиты были объединены единым умыслом, направленным на нарушение авторских прав и использование вредоносных средств, и полностью охватывались составом ст. 273 УК РФ в совокупности со ст. 146 УК РФ.

Наложение составов на практике происходит в ситуациях, когда неправомерный доступ является не самоцелью, а способом или этапом для последующего использования или распространения вредоносных программ либо нарушения исключительных прав, что требует от судов четкого установления конечной цели деяния и основной направленности умысла виновного для точной квалификации.

Таким образом, последовательная оценка трех обстоятельств является путем разграничения ст. 272 УК РФ и ст. 273 УК РФ. Во-первых, необходимо установить

---

[251] Кассационное постановление Седьмого кассационного суда общей юрисдикции от 9 октября 2024 г. по делу № 7У-5887/2024[77-3247/2024] [Электронный ресурс]. – Доступ из СПС «Гарант».
[252] Апелляционное постановление Оренбургского областного суда от 17 ноября 2016 г. по делу № 22-4323/2016 [Электронный ресурс]. – Доступ из СПС «Гарант».

сам факт несанкционированного доступа. Во-вторых, выяснить, использовалась ли вредоносная программа как орудие деструктивного воздействия. В-третьих, определить взаимосвязь между использованием вредоносной программы и несанкционированным доступом. Если вредоносная программа не применялась, деяние квалифицируется только по ст. 272 УК РФ. Если программа использовалась, а доступ являлся лишь техническим этапом, не имеющим самостоятельной ценности, содеянное полностью охватывается ст. 273 УК РФ без дополнительной квалификации по ст. 272. Но в случаях, когда доступ был получен самостоятельно, независимо от последующего использования вредоносной программы, требуется квалификация по совокупности обеих статей. Данный подход, который основан на анализе судебной практике, который позволит единообразно решать вопросы квалификации.

Следующий дискуссионный вопрос в контексте проблем квалификации возникает из соотношения ст. 138^1 УК РФ, регламентирующей ответственность за незаконный оборот специальных технических средств, предназначенных для негласного получения информации, и ст. 273 УК РФ.

В ходе анализ судебной практики не встречались дела, где программное обеспечение, которое является специальным техническим средством, одновременно выявлялся вредоносный код, с учетом этого, данное обстоятельство нуждается в доктринальном восполнении. Так как схожесть объективной стороны во внешнем проявлении могут создавать потенциальный риск уголовно-правовых норм.

В этом отношении следует признать, что высказанная в уголовно-правовой доктрине позиция Е.Г. Усова, согласно которой программное обеспечение в силу своей нематериальной природы не может быть отнесено к категории технических средств, а его создание для негласного получения информации должно квалифицироваться исключительно как создание вредоносной программы по ст.

273 УК РФ, является спорной[253]. Действительно, программа как совокупность данных и команд не имеет физического субстрата, однако данное обстоятельство не предопределяет автоматически ее вредоносный характер.

Если смотреть только на форму, в которой существует объект, но не рассматривать его функциональное содержание, тогда сфера действия ст. 273 УК РФ будет неоправданно расширяться, что приведет размыванию границ состава. Допустим, программное обеспечение, где основной целью является скрытное получение информации, но при этом в ее коде отсутствуют средства нейтрализации штатных систем защиты компьютерной информации и не предназначено для несанкционированного уничтожения, блокирования, модификации или компьютерной информации, не отвечает признакам вредоносной программы в том значении, которое придается этому понятию в ст. 273 УК РФ.

Таким образом, принципиальное значение имеет установление того факта, что центральным элементом состава преступления, предусмотренного ст. 273 УК РФ, является не цель негласного получения сведений и не форма существования предмета преступления, а исключительно вредоносный характер программы, выражающийся в ее способности к деструктивному воздействию на компьютерную информацию или средства ее защиты. В случае если для обеспечения негласного получения информации виновный создает, использует или распространяет программное обеспечение, обладающее функционалом вредоносной программы, т.е. содержащее алгоритмы, предназначенные для преодоления средств защиты, модификации или уничтожения данных, содеянное подлежит квалификации по совокупности преступлений, что прямо предусмотрено п. 16 постановления Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37[254].

---

[253] См.: Усов Е.Г. Уголовная ответственность за незаконный оборот специальных технических средств, предназначенных для негласного получения информации : дис. ... канд. юрид. наук. Иркутск, 2020. С. 70.

[254] 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». URL: https://www.consultant.ru/document/cons_doc_LAW_434573/ . (дата обращения: 17.04.2026).

Сложности также возникают в связи с проблемным аспектом субъективной стороны преступления. Для привлечения к ответственности по ст. 273 УК РФ правоприменителю необходимо достоверно установить наличие прямого умысла на создание, использование или распространение вредоносной программы именно в целях причинения вреда компьютерной информации, системе или самой инфраструктуре. Однако на практике доказывание такой цели сопряжено со значительными трудностями, что обусловлено прежде всего технической сложностью и неочевидностью мотивации действий в цифровой среде.

Программы двойного назначения создают особую проблему. Само по себе использование таких программ не является противоправным, а преступный характер действий зависит от умысла и цели, с которой такая программа применяется. В результате возникает серьезная квалификационная проблема, необходимо отграничить умышленное преступное деяние, например от правомерной деятельности специалиста по информационной безопасности. Как показывает практика, крайне сложно установить умысел, особенно в случаях с программами, которые обладают легитимным функционалом.

Анализ судебной практики демонстрирует два разных подхода к разрешению коллизии. Например, первый подход отражен в решении по делу Забелина[255] и определении по делу Зюкина[256], который характеризуется формально-объективированным установлением умысла. Факт осуществления обвиняемым деяний по распространению или использованию модифицированного программного обеспечения, технически предназначенного для нейтрализации средств защиты, в совокупности с корыстным мотивом (получение денежного вознаграждения) является достаточным доказательством наличия прямого умысла, в связи с этим суды оставили обвинительные приговоры в силе. Умысел презюмируется из характера действий и их результата.

---

[255] См.: Постановление Первого кассационного суда общей юрисдикции от 19 апреля 2023 г. по делу № 7У-2934/2023[77-1806/2023] [Электронный ресурс]. – Доступ из СПС «Гарант».

[256] См.: Кассационное определение СК по уголовным делам Первого кассационного суда общей юрисдикции от 16 мая 2024 г. по делу № 77-1910/2024 [Электронный ресурс]. – Доступ из СПС «Гарант».

Так, в деле Забелина ключевым доказательством являлось заключение экспертизы, которое установило наличие в игровой приставке программного кода, который позволял обходить техническую защиту и осуществлять несанкционированную модификацию, а также его неоднократное использование. Тоже самое экспертизой было установлено в деле Зюкина. Таким образом, в рамках данного подхода акцент смещается с субъективного внутреннего убеждения обвиняемого на объективные последствия его действий и их экспертную интерпретацию, что упрощает задачу обвинения, но создает риск объективного вменения.

Второй подход, детально обоснованный в апелляционном определении Верховного Суда Республики Крым[257], напротив, демонстрирует самостоятельное формирование преступного умысла. После проведения тщательного анализа фактических обстоятельств у обвиняемого субъективной составляющей, суд оставил в силе оправдательный приговор. Было установлено, что до обращения оперативного сотрудника у лица отсутствовали как сами вредоносные программы, так и умысел на их использование. Ключевым фактом для суда стало нарушение процедуры ОРМ: постановление о проведении «проверочной закупки» было вынесено после того, как оперативник, действуя под легендой, инициировал контакт и сформулировал заказ на установку конкретного нелицензионного программного обеспечения. Суд квалифицировал эти действия не как проверку имеющейся информации о противоправной деятельности, а как провокацию, запрещенную ст. 5 Федерального закона «Об оперативно-розыскной деятельности»[258], поскольку они фактически сформировали у лица умысел, которого ранее не было. Данный подход демонстрирует высокий стандарт доказывания для обвинения, который требует подтверждения независимого от действий правоохранителей источника и зрелости преступного намерения.

---

[257] Апелляционное определение СК по уголовным делам Верховного Суда Республики Крым от 3 сентября 2024 г. по делу № 22-2322/2024 [Электронный ресурс]. – Доступ из СПС «Гарант».
[258] Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» // СЗ РФ. 1995. № 33. Ст. 3349.

Как мы можем заметить, что в части доказывания субъективной стороны судебная практика свидетельствует о недостаточном определении критериев доказывания и противоречивости, думается, что все это создает угрозу как необоснованного привлечения к ответственности лиц, не осознававших вредоносной сущности своих действий, особенно при работе с программами двойного назначения, так и невозможности эффективного преследования реальных злоумышленников из-за формальных процессуальных нарушений при проведении ОРМ.

§ 2. Основные направления совершенствования уголовного законодательства Российской Федерации и Кыргызской Республики об ответственности за создание, использование и распространение вредоносных компьютерных программ

Совершенствование уголовно-правовых норм, направленных на противодействие использованию вредоносных компьютерных программ, является одной из наиболее актуальных задач для национальных законодательств в условиях глобальной цифровизации. Динамичное развитие информационных технологий, с одной стороны, создает новые возможности для социально-экономического прогресса, а с другой – порождает ранее неизвестные формы общественно опасных деяний, требующие адекватного правового реагирования.

Уголовные законодательства Российской Федерации и Кыргызской Республики, содержащие составы преступлений, связанных с созданием, использованием и распространением вредоносного программного обеспечения, формировались в ответ на вызовы времени. Однако непрерывная эволюция киберугроз, усложнение методов атак и трансграничный характер данной преступности обуславливают необходимость постоянного анализа и развития этих правовых институтов.

В этой связи сравнительное исследование основных направлений совершенствования отечественного и кыргызского уголовного законодательства в

указанной сфере представляется важным для выработки эффективных механизмов защиты информационной безопасности, как на национальном, так и на региональном уровне, учитывая общность многих стоящих перед двумя странами проблем в киберпространстве.

Сравнительный анализ признаков объекта и предмета ст. 273 УК РФ и 320 УК КР, проведенный в § 1 гл. 2 настоящего исследования, в результате которого можно сделать вывод о том, что в качестве предмета ст. 273 УК РФ рассматривает вредоносную компьютерную программу и иную вредоносную компьютерную информацию, то ст. 320 УК КР ограничивается лишь вредоносным программным продуктом.

В этой связи представляется обоснованным положение о необходимости расширения предмета ст. 320 УК КР путем включения в него понятия «цифровая компьютерная информация». Данная позиция подкрепляется рядом аргументов.

Во-первых, сам законодатель Кыргызской Республики уже оперирует понятием «компьютерной информации» в смежных нормах, в частности в ст. 319 УК КР, посвященной несанкционированному доступу, что свидетельствует о признании данного явления правовым полем и устраняет терминологические барьеры для имплементации.

Во-вторых, как справедливо отмечают ученые[259], иная вредоносная компьютерная информация, не представляющая собой законченную самостоятельную программу, способна, взаимодействуя с полезными кодами, дестабилизировать и негативно влиять на их функционирование, причиняя тем самым существенный вред охраняемым законом интересам.

Таким образом, существующая формулировка ст. 320 УК КР, которая игнорирует этот широкий пласт вредоносных воздействий, создает опасный пробел в уголовно-правовой защите информационной безопасности. Ведь, ограничение предмета лишь программными продуктами не соответствует современным реалиям

[259] Грачева Ю.В., Чучаев А.И. Указ. соч. С. 319–320; Дворецкий М.Ю. Корреляции главы 28 УК РФ в контексте оптимизации уголовной ответственности и повышения эффективности правоприменительной практики // Вестник ТГУ. 2012. № 6. С. 266–271.

киберугроз, где вредоносная информация может выполнять деструктивные функции без образования отдельной программы.

Следовательно, для обеспечения адекватного и технологически нейтрального уголовно-правового реагирования на эволюционирующие киберугрозы предмет ст. 320 УК КР должен быть расширен по модели ст. 273 УК РФ и включать наряду с вредоносным программным продуктом также иную вредоносную компьютерную информацию, что будет способствовать повышению эффективности правоприменительной практики в сфере противодействия компьютерной преступности, а также унификации подходов.

Отсутствие легальных дефиниций ключевых понятий «вредоносная компьютерная программа» и «вредоносный программный продукт» является наиболее существенной проблемой в правоприменении, как показывает проведенный анализ. Соответствующие термины используются в диспозициях ст. 273 УК РФ и ст. 320 УК КР, однако их содержательное наполнение остается недостаточно раскрытым, что приводит к снижению эффективности уголовно-правового противодействия.

В целях единого понимания предлагается законодательно закрепить данные определения. Думается, что логичным и практичным способом для этого было бы введение специального примечания, в котором следует исчерпывающе прописать признаки вредоносности, включая предназначенность программы для несанкционированного уничтожения, блокирования, модификации, копирования информации или нейтрализации средств защиты, а также отдельно оговорить статус инструментов, используемых в правомерных целях обеспечения безопасности информационных систем, исключив их из-под действия уголовного запрета.

Следующей существенной проблемой, выявленной в доктрине уголовного права, является дефект законодательной техники в конструкции диспозиций, порождающий неоднозначность толкования.

Как справедливо отмечают исследователи, в частности К.Н. Евдокимов[260] и Т.Л. Тропина[261], при описании объективной стороны преступления, предусмотренного ст. 273 УК РФ, законодатель использовал формулировки во множественном числе «создание, распространение или использование вредоносных компьютерных программ». Если буквально прочесть настоящую норму, то можно прийти к абсурдному выводу, что уголовная ответственность наступает лишь при совершении действий в отношении двух или более вредоносных программ, однако, совершено точно, что создание, распространение или использование даже одной такой программы представляет не меньшую общественную опасность.

Аналогичная терминологическая неточность, присутствует и в уголовном законодательстве Кыргызской Республики, где ст. 320 УК КР также оперирует понятием «программных продуктов» во множественном числе, которая в последующем может создавать почву для судебных ошибок,

Целесообразно, по нашему мнению, сформулировать описание объективной стороны, исключив употребление множественного числа. При этом использовать нейтральные формулировки, которые охватывали бы как единичный, так и множественный объект посягательства, например, «создание программного продукта (компьютерной программы) или внесение изменений в существующий программный продукт, а равно использование или распространение такого программного продукта (такой компьютерной программы)…». Данное предложение будет способствовать единообразному и правильному применению уголовного закона на практике как в Российской Федерации, так и в Кыргызской Республике.

На протяжении длительного времени в доктрине уголовного права высказывается последовательная критика в действующем уголовном законодательстве существенного пробела. Как отмечает В.Г. Степанов-Егиянц,

---

[260] См.: Евдокимов К.Н. Противодействие компьютерной преступности: теория, законодательство, практика: дис. ... д-ра юрид. наук. М., 2021.С. 398–399.
[261] Тропина Т.Л. Указ. соч. С. 178.

отсутствие в диспозиции ст. 273 УК РФ таких деяний, как приобретение и (или) хранение вредоносных программ, является труднообъяснимым, особенно на фоне криминализации их распространения и использования[262]. Возникает следующая ситуация, когда лицо, целенаправленно покупает вирус для последующего применения, получается, что формально не подпадает под действие уголовного закона до момента начала активных действий по его использованию или распространению.

В пользу криминализации приобретения и (или) хранения аргументы строится на нескольких взаимосвязанных моментах. В первую очередь, как подчеркивает В.Ю. Максимов[263], данное требование вытекает из логической структуры объективной стороны преступлений, связанных с обращением с источниками повышенной опасности. Так как невозможно без установления запрета на все ключевые стадии оборота осуществлять полноценный и эффективный контроль на таким опасным предметом.

Во-вторых, сам факт нахождения вредоносной программы в незаконном владении создает постоянную угрозу безопасности информационных систем, в связи с тем, что такое владение, как правило, является подготовительным этапом для совершения более тяжких преступлений.

В-третьих, К.Н. Евдокимов аргументирует это тем, что большинство компьютерных преступников не являются создателями вирусов, а целенаправленно приобретают готовые вредоносные продукты на специализированных сетевых ресурсах[264]. Поэтому криминализация приобретения будет способствовать перекрытию каналов снабжения преступников вредоносным инструментом.

Как верно, уточняет Е.А. Маслакова, ответственность должна наступать не за любое приобретение или хранение, а лишь за те из них, которые совершены с

---

[262] См.: Степанов-Егиянц В.Г. Методологическое и законодательное обеспечение безопасности компьютерной информации в Российской Федерации : уголовно-правовой аспект : дис. ... д-ра юрид. наук. М., 2016. С. 275–276.

[263] См.: Максимов В.Ю. Указ. соч. С. 10.

[264] См.: Евдокимов К.Н. Противодействие компьютерной преступности: теория, законодательство, практика: дис. ... д-ра юрид. наук. М., 2021. С. 134–135.

конкретной целью[265]. Безусловно, настоящий подход позволяет провести аналогию с правовым режимом оборота оружия, наркотиков или взрывчатых веществ, где сами действия по незаконному приобретению и хранению образуют самостоятельные составы преступлений в силу их высокой потенциальной опасности.

Дополнение диспозиций соответствующих ст. 273 УК РФ и ст. 320 УК КР деяниями по приобретению и (или) хранению вредоносной компьютерной программы или вредоносной компьютерной информации подтверждается мнением большинства ученых относительно данного вопроса. Предлагаемое расширение объективной стороны состава преступления является логичным развитием уголовно-правовой политики в сфере защиты информационной безопасности, направленной на установление контроля над всем циклом обращения цифровых источников повышенной опасности.

Проведенное нами социологическое исследование показало, что 58% респондентов поддерживают инициативу, связанную с криминализацией приобретения и (или) хранения вредоносных компьютерных программ в целях совершения иного преступления. Еще 29% опрошенных выразили частичную поддержку, в связи с возможными опасениями относительно сложностей доказывания преступной цели на практике. Примечательно, что лишь 12,9% респондентов не поддержали данное предложение, мотивируя это риском необоснованного привлечения к ответственности за так называемое пустое хранение, которое связано, например, с изучением вредоносного кода[266].

Другим дискуссионным вопросом, уже давно обсуждаемым в научной доктрине, является проблема разграничения уголовно наказуемого и правомерного оборота программ, обладающих техническими признаками вредоносности.

Как уже было отмечено, вредоносность программы – это не ее сугубо техническая функция, а юридическая характеристика, определяемая

---

[265] См.: Маслакова Е.А. Незаконный оборот вредоносных компьютерных программ: уголовно-правовые и криминологические аспекты : дис. ... канд. юрид. наук. М., 2008. С. 11.

[266] Результаты опроса в Приложении № 1 к диссертации.

предназначением и умыслом лица. Один и тот же программный код может быть легальным кибероружием, созданным по заказу государства для ведения оборонительных или разведывательных операций, и нелегальным инструментом хакерской атаки. Разница – не в коде, а в правовом статусе создателя, цели создания и наличии/отсутствии разрешения.

В России и Кыргызстане, однако, отсутствует правовое регулирование создания и оборота «кибероружия» – программ, обладающих функционалом несанкционированного воздействия на цифровую инфраструктуру, разрабатываемых для нужд обороны, безопасности, контртеррористических операций или научных исследований. Нет ни законов, ни подзаконных актов, которые определяли бы, кто, на каком основании и в каком порядке может создавать, хранить и использовать такое специальное программное обеспечение в легальных целях. В результате любое создание подобного кода (даже для нужд Минобороны) формально подпадает под действие уголовно-правового запрета.

Это, по сути, абсурдная правовая ситуация. Получается, что страна, которая нуждается в защите от киберугроз, сама криминализирует деятельность по созданию средств такой защиты. Необходимо четкое разделение: легальный статус программ, обладающих функционалом несанкционированного воздействия на цифровую инфраструктуру (для государственных нужд, научных исследований, тестирования безопасности) и нелегальный – всё, что выходит за эти рамки.

Международное право учитывает эту проблему. В п. 2 ст. 11 Конвенции ООН против киберпреступности 2025 г. прямо указано, что уголовная ответственность не должна наступать в тех случаях, когда действия с вредоносными программами не преследуют цели совершения преступления, а связаны, например, с разрешенным тестированием или защитой информационной системы[267]. Как справедливо отмечают исследователи, не любое создание, использование или

[267] Резолюция Генеральной Ассамблеи ООН A/RES/79/243 от 24 декабря 2024 г. // Официальный сайт ООН. URL: https://docs.un.org/ru/A/RES/79/243 (дата обращения 20.12.2025).

распространение, приводящее к блокированию, модификации или уничтожению информации, должно влечь уголовную ответственность[268].

Существует широкий спектр общественно полезной и легитимной деятельности, которая связана с подобными программами. К таковой относится работа специалистов по информационной безопасности, которые занимаются разработкой или анализом свойств вредоносных программ обеспечение для создания антивирусных средств. Следовательно, действующие же формулировки ст. 273 УК РФ и ст. 320 УК КР, в которых отсутствуют указания на противоправность деяния, создают потенциальную возможность для криминализации такой необходимой профессиональной деятельности.

В этой связи представляется обоснованной и своевременной позиция ученых, предлагающих уточнить законодательство путем введения признака незаконности. Необходимо согласиться с мнением В. Г. Степанова-Егиянца о том, что наиболее последовательным решением было бы изложение диспозиций, начав их со слова «незаконные»[269], как предлагает М.М. Малыковцев[270], либо сформулировать название ст. 273 УК РФ как «Незаконный оборот вредоносных программ», по аналогии с решением Е.А. Маслаковой[271].

Данный подход в полной мере применим и к ст. 320 УК КР, поскольку проблема носит универсальный характер. Внесение такого изменения позволило бы четко отделить преступное поведение от правомерных действий в сфере кибербезопасности, обеспечив тем самым баланс между интересами защиты информационных систем и необходимостью свободного развития защитных технологий, и привело бы уголовные нормы в соответствие с реалиями современного цифрового мира.

---

[268] См.: Степанов-Егиянц В.Г. Указ. соч. С. 273; Малыковцев М. М. Указ. соч. С. 86.
[269] См.: Степанов-Егиянц В.Г. Указ. соч. С. 273–274.
[270] См.: Малыковцев М. М. Указ. соч. С. 88.
[271] См.: Маслакова Е.А. Незаконный оборот вредоносных компьютерных программ: уголовно-правовые и криминологические аспекты : дис. ... канд. юрид. наук. М., 2008. С. 104.

Проведенное нами социологическое исследование показало, что большинство специалистов поддерживают необходимость законодательного разграничения преступной деятельности и профессионального функционала в сфере информационной безопасности. Так, 68,9% респондентов убеждены, что диспозиции статей необходимо дополнить указанием на незаконный характер деяний, начав их изложение со слова «незаконные...», чтобы избежать риска привлечения к ответственности специалистов по информационной безопасности, действующих в рамках правомерного тестирования на проникновение. Еще 13,1% опрошенных поддержали эту идею с оговоркой о необходимости одновременного законодательного закрепления конкретных случаев правомерного использования вредоносных программ, например, в рамках киберучений, в то время как только 18% сочли данное уточнение избыточным[272].

Одним из дискуссионных моментом является наличие в диспозиции кыргызской нормы действия «внесение изменений», которое было исключено российским законодателем из ст. 273 УК РФ в 2011 г. Существующий пробел порождает сложности в правоприменении, что становится особенно очевидным при рассмотрении современных реалий киберпреступности, где преимущественно используется не отдельные вредоносные программы, а целые их семейства, основанные на общем базовом коде и подвергающиеся постоянным модификациям. Данное исследование, пожалуй, ставит целью аргументировать необходимость возвращения в объективную сторону состава преступления, предусмотренного ч. 1 ст. 273 УК РФ, действия по «внесению изменений во вредоносную программу».

Ярким примером является история вируса-вымогателя Petya, созданного под псевдонимом Janus[273]. Изначально он был инструментом для получения финансовой выгоды по модели “Malware-as-a-Service”. Но позднее его базовый код был использован и существенно модифицирован другими лицами для создания

---

[272] Результаты опроса в Приложении № 1 к диссертации.

[273] См.: Автор оригинального вируса-вымогателя Petya опубликовал главный ключ расшифровки. URL: https://www.bleepingcomputer.com/news/security/author-of-original-petya-ransomware-publishes-master-decryption-key/ (дата обращения: 05.01.2026).

деструктивной версии NotPetya в 2017 г., что вызвало публичное осуждение со стороны оригинального автора[274].

Еще более показательным примером является обнаруженная специалистами ESET в 2025 г. модифицированная версия HybridPetya, которая, унаследовав черты предшественников, обрела новые опасные свойства, такие как способность обходить механизм UEFI Secure Boot[275]. Все эти случаи наглядно демонстрируют, что значительная часть современной киберпреступной деятельности заключается не в создании вредоносных программ «с нуля», а в целенаправленном изменении и адаптации уже существующего кода под новые цели, при этом эксплуатируя новейшие уязвимости.

Именно в данном контексте приобретает весомую научную и практическую значимость позиция К. Н. Евдокимова, который обосновывает логичность возвращения в объективную сторону ст. 273 УК РФ действия в виде «внесение изменений»[276]. Аргументация настоящей позиции строится на том, что в нынешних условиях автор конкретной модификации должен нести ответственность именно за создание, использование и распространение своей производной версии, а не за базовый код, написанный другими лицами.

Таким образом, проведенный анализ, с существующими примерами эволюции реальных вредоносных семейств и мнением ученых, убедительно свидетельствует о наличии в действующей редакции ст. 273 УК РФ существенного пробела. Исключение из объективной стороны состава преступления действия «внесение изменений в компьютерную программу» не соответствует реалиям современной киберпреступности. Возвращение данного признака в диспозицию ч. 1 ст. 273 УК РФ, как обоснованно предлагает К.Н. Евдокимов, представляется

---

[274] См.: NotPetya: червь на десять миллиардов долларов. URL: https://www.dna.fi/dnabusiness/blogi/-/blogs/notpetya-the-ten-billion-dollar-worm (дата обращения: 05.01.2026).

[275] См.: Представляем HybridPetya: аналог Petya/NotPetya с обходом защиты UEFI Secure Boot. URL: https://www.welivesecurity.com/en/eset-research/introducing-hybridpetya-petya-notpetya-copycat-uefi-secure-boot-bypass/ (дата обращения: 05.01.2026)

[276] См.: Евдокимов К.Н. Противодействие компьютерной преступности: теория, законодательство, практика: дис. ... д-ра юрид. наук. М., 2021. С. 326–327.

логичным и необходимым шагом для обеспечения адекватного уголовно-правового реагирования[277].

Результаты социологического исследования, проведенного нами показывает, что 40% респондентов считают данное предложение обоснованным. Однако значительная доля опрошенных – 36,7% оценивать инициативу как спорную, аргументируя это тем, что «внесение изменений» по своей сути может рассматриваться как разновидность создания или модификации вредоносной программы. Лишь 15% респондентов считают, что возвращение данного признака излишним, полагая, что действующая редакция с формулировками «создание, использование, распространение» и так охватывает все необходимые действия, а 8,3% затруднились с ответом. Несмотря на определенную дискуссионность вопроса в профессиональной среде, наличие весомой доли сторонников конкретизации объективной стороны свидетельствует о целесообразности возвращения в диспозицию ч. 1 ст. 273 УК РФ действия «внесение изменений», что в большей степени соответствует структуре современной киберпреступной деятельности, основанной на постоянной модификации существующего вредоносного кода[278].

В научной среде одним из наиболее обсуждаемых и требующих законодательного осмысления является предложение о криминализации создания и обеспечения функционирования информационных ресурсов, заведомо предназначенных для распространения вредоносных компьютерных программ или иной информации, необходимой для их функционирования. Данная инициатива обусловлена стремительной эволюцией форм организованной преступной деятельности в цифровой среде, которая, как отмечается в современных исследованиях, переходит к формированию сложных сетевых структур и экосистем.

---

[277] См.: Евдокимов К.Н. Противодействие компьютерной преступности: теория, законодательство, практика: дис. ... д-ра юрид. наук. М., 2021. С. 399.

[278] Результаты опроса в Приложении № 1 к диссертации.

По мнению В.В. Полякова, который анализирует цифровую трансформацию организованной преступности, приходит к выводу о формировании экосистем преступных сообществ, представляющих собой сетевые объединения автономных групп, взаимодействующих посредством цифровых платформ в сети Даркнет, что является качественно новым и крайне опасным явлением. Технологической основой таких экосистем выступают именно цифровые платформы, которые создают теневую информационную среду, объединяющую сетевые сервисы и ресурсы для совместной преступной деятельности[279].

Пожалуй, обоснованно указывают Р.И. Дремлюга и А.И. Коробеев, что создание и обеспечение работы сетевых платформ для осуществления преступной деятельности посягает на основы цифровой экономики и информационного общества, которая обладает высокой степенью общественной опасности и не может рассматриваться как простое соучастие в преступлениях, что подтверждает необходимость его криминализации в качестве самостоятельного состава преступления[280].

Актуальность и масштабность данной проблемы подтверждаются не только научным анализом, но и данными мониторинга теневого сегмента Интернета.

Так, компания «Лаборатория Касперского» в своем исследовании фиксирует двукратный рост объявлений о найме в криминальном Даркнете за последние три года, что свидетельствует о профессионализации и индустриализации киберпреступности, где разработка вредоносного программного обеспечения и сопутствующих сервисов становится одной из наиболее востребованных специальностей. Исследование компании “F6”, в свою очередь, наглядно демонстрирует наличие сформировавшегося рынка криминальных услуг в

---

[279] См.: Поляков В. В. Формирование экосистем преступных сообществ как следствие цифровой трансформации организованной преступной деятельности // Вестник Томского государственного университета. 2025. № 511. С. 230.

[280] См.: Дремлюга Р. И., Коробеев А. И. Уголовно-правовая политика в сфере противодействия платформизации преступной деятельности // Всероссийский криминологический журнал. 2022. Т. 16. № 1. С. 53–54.

Дарквебе, где можно приобрести не только сами вредоносные программы и доступ к корпоративным сетям, но и целые комплекты для проведения атак[281].

Существующая судебная практика по ст. 273 УК РФ, к сожалению, не отражает всей глубины проблемы, так как направлена на привлечение к ответственности конечных исполнителей, непосредственно использующих вредоносные программы.

Анализ приговоров, например, по делам Новика (ч. 2 ст. 273 УК РФ, распространение и использование ПО “RisePro” группой лиц)[282], Чернова (ч. 2 ст. 273 УК РФ, использование фишинговых ботов для кражи аккаунтов Telegram)[283], а также Большакова (ч. 2 ст. 273 УК РФ, создание и распространение через чат-бота программы для нейтрализации средств защиты[284]) показывает, что лица, создающие и администрирующие сами платформы-магазины приложений, форумы для обмена инструментами или сервисы по аренде инфраструктуры для атак, в орбиту уголовного преследования попадают крайне редко.

Чаще всего, как в деле Халимова, действия обвиняемых квалифицируются по совокупности преступлений (неправомерный доступ, мошенничество), а роль создателя платформы (в данном случае Telegram-канала с инструкциями и ботами для получения данных) остается за рамками предъявленного обвинения[285]. Даже в таком масштабном деле, как дело Ахметшина, где фигурирует создание закрытой группы “Luxury Mafia” в Telegram для координации действий участников и распространения ссылок на вредоносное программное обеспечение, ответственность организатора группы (установленного лица № 1) и создателя вредоносной программы («кодера») рассматривается в рамках соучастия в

---

[281] См.: Даркнет (теневой интернет, DarkNet). URL: https://www.tadviser.ru/index.php/_DarkNet (дата обращения: 05.03.2026).

[282] Приговор Химкинского городского суда Московской области от 11 сентября 2025 г. по делу № 1-639/2025 [Электронный ресурс]. – Доступ из СПС «Гарант».

[283] Приговор Свердловского районного суда г. Костромы Костромской области от 12 ноября 2025 г. по делу № 1-364/2025 [Электронный ресурс]. – Доступ из СПС «Гарант».

[284] Приговор Железнодорожного районного суда г. Красноярска Красноярского края от 6 ноября 2025 г. по делу № 1-312/2025 [Электронный ресурс]. – Доступ из СПС «Гарант».

[285] Приговор Магаданского городского суда Магаданской области от 3 октября 2025 г. по делу № 1-500/2025 [Электронный ресурс]. – Доступ из СПС «Гарант».

конкретных преступлениях (мошенничестве, неправомерном доступе), а не за сам факт создания и поддержания этой криминальной платформы[286]. Это создает ситуацию, когда организаторы преступных онлайн-площадок, выступающие ключевым звеном современных киберпреступных экосистем, остаются вне поля действия уголовного закона, что существенно снижает эффективность борьбы с данным явлением.

В связи с изложенным представляется обоснованным и своевременным предложение о криминализации в ст. 273 УК РФ и ст. 320 УК КР деяний, выражающихся в создании и (или) обеспечении функционирования информационного ресурса (сайта в сети «Интернет» и (или) страницы сайта в сети «Интернет»), заведомо предназначенного для незаконных хранения, передачи (распространения, предоставления, доступа) цифровой информации, заведомо предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств ее защиты.

Даже несмотря на то что эмпирические данные, напрямую отражающие масштаб данного конкретного деяния, могут быть ограничены в силу высокой латентности и специфики объекта исследования, предлагаемая норма представляется упреждающей мерой, направленной на нейтрализацию ключевого элемента современных киберпреступных экосистем.

Более того, результаты проведенного нами социологического опроса свидетельствуют о том, что большинство респондентов сталкиваются с проблемами при квалификации действий лиц, создающих инфраструктуру для распространения вредоносного программного обеспечения, и поддерживают необходимость введения специализированной уголовной ответственности за подобные деяния.

---

[286] Приговор Нижневартовского городского суда Ханты-Мансийского автономного округа – Югры от 27 августа 2025 г. по делу № 1-1231/2025 [Электронный ресурс]. – Доступ из СПС «Гарант».

Таким образом, предлагаемое дополнение уголовного законодательства России и Кыргызстана не только отвечает современным вызовам и тенденциям развития киберпреступности, подтвержденным научными исследованиями и аналитическими отчетами, но и находит эмпирическое подтверждение своей востребованности в правоприменительной среде, что в совокупности делает его своевременным и практически значимым шагом в деле совершенствования уголовно-правового противодействия преступлениям в сфере компьютерной информации.

И наконец, в завершение следует указать на еще одно перспективное направление возможного совершенствования уголовного законодательства России и Кыргызстана в части установления ответственности за действия с вредоносными компьютерными программами. Таковым является обсуждаемая многими проблема появления вредоносных цифровых программ, построенных на основе технологий ИИ.

Традиционное вредоносное программное обеспечение (вирусы, трояны, программы-вымогатели) характеризуется статичным кодом: его поведение предопределено создателем. ИИ же наделяет вредоносные программы тремя принципиально новыми свойствами. Во-первых, это адаптивность – способность самостоятельно видоизменяться, обходить сигнатурные методы защиты и выбирать наиболее уязвимые цели. Во-вторых, встроенный ИИ позволяет осуществлять тотальную социальную инженерию: генерировать идеально правдоподобные фишинговые письма, голосовые сообщения и даже видеозвонки с использованием технологии дипфейк (как в случае с министром обороны Италии в 2025 г.). В-третьих, появился класс так называемых «вредоносных GPT» (например, GhostGPT) – специализированных ИИ-чат-ботов без цензуры, которые сами пишут вредоносный код по запросу пользователя[287]. Таким образом,

[287] См.: Взлом с использованием ИИ: типы киберпреступлений с использованием ИИ и способы обезопасить себя. URL: https://www.kaspersky.ru/resource-center/preemptive-safety/ai-cybercrime (дата обращения: 12.06.2026).

возникает ситуация «мета-оружия», когда один ИИ-инструмент создает тысячи других вариаций вредоносных программ.

Например, особое внимание заслуживает Кыргызская Республика, которая уже сделала важный шаг в признании новых технологических угроз на уровне цифрового законодательства. Так, в п. 15 ст. 1 Цифрового кодекса Кыргызской Республики закреплено легальное определение дипфейка – это создание или изменение изображений или аудио, видеоматериалов, демонстрирующих значительное сходство с существующими лицами, объектами, явлениями или событиями и способных создать у физических лиц ложное впечатление о достоверности таких изображений или материалов[288].

В этой связи, как правило, делается акцент на том, что такую вредоносную программу будет отличать уже не просто инструментальный статус орудия совершения конкретного посягательства, а существенная автономность, самообучаемость, адаптивность к мерам противодействия и средствам защиты, вариативность (или даже непредсказуемость) действия и, как следствие, значительно большая эффективность. Иными словами, ИИ-вредоносная компьютерная программа собой практически может заменить сложное соучастие в совершении преступления.

Р.И. Дремлюга справедливо выделяет еще и такое свойство системы искусственного интеллекта, как ее интеллектуальность – способность имитировать деятельность человека, что, по мнению автора, безусловно указывает на более высокую общественную опасность преступного деяния[289].

В российской теории уголовного права также отмечается, что, обладая большими массивами данных, современные нейронные сети ИИ зачастую превосходят человека в решении многих задач[290].

---

[288] Кодекс КР от 31 июля 2025 г. № 178 «Цифровой Кодекс Кыргызской Республики» https://cbd.minjust.gov.kg/3-48/edition/35412/ru?lang=ru (дата обращения: 13.06.2026).

[289] См.: Дремлюга Р. И. Уголовно-правовая охрана цифровой экономики и информационного общества от киберпреступных посягательств: доктрина, закон, правоприменение: монография. М., 2022. С. 247.

[290] См.: Грачева Ю.В., Иванов С. А., Маликов С. В., Чучаев А. И. Риски цифровизации: виды, характеристика, уголовно-правовая оценка: монография / отв. ред. Ю. В. Грачева. М., 2022. С. 9.

Полагаем, что в этом отношении уголовное законодательство не только России и Кыргызстана, но и всех стран потребует вполне конкретных законодательных мер в части дифференциации уголовной ответственности за создание, использование и распространение таких вредоносных цифровых ИИ-агентов. Надо признать, что как российская доктрина, так и теория уголовного права Кыргызстана в этом аспекте довольно слабо разработаны. Проблема не только не раскрыта, но и толком не поставлена. Думается, что объясняется это отсутствием социальных предпосылок – современные правоохранительные органы еще не сталкивались с вредоносными ИИ-агентами. Однако многое указывает на то, что это лишь вопрос будущего, причем уже не столь отдаленного.

ЗАКЛЮЧЕНИЕ

Проведенное нами сравнительно-правовое диссертационное исследование позволило сделать теоретические выводы и сформулировать следующие положения.

Во-первых, установлено, что одним из приоритетных направлений национальной безопасности обоих государств является информационная безопасность. Об этом свидетельствуют существующие стратегические документы и уголовно-правовая политика Российской Федерации и Кыргызской Республики, которая находится на стадии активного развития в области противодействия киберпреступности.

Во-вторых, Российская Федерация и Кыргызская Республика прошла несколько этапов эволюции уголовного законодательства в сфере компьютерных преступлений: от криминализации первоначальных базовых составов в конце 1990 гг. и до появления специальных норм о защите критической информационной инфраструктуры, средств доступа, персональных данных на современном этапе, который характеризуется дифференциацией ответственности. Безусловно, в Российской Федерации наблюдается более динамичное развитие главы 28 УК РФ, которая существенно расширила перечень составов преступлений, в то время как, Кыргызская Республика сохранила более лаконичную структуру главы 40 УК КР.

В-третьих, анализ международного опыта в данной сфере демонстрирует определенный вектор развития глобального сотрудничества. Историческим событием в международном правовом поле является принятие Конвенции ООН против киберпрепреступности, которая сформирует универсальную правовую основу для борьбы с киберугрозами. Сравнительный анализ норм уголовного законодательства России и Кыргызстана с положениями Конвенции ООН против киберпреступности показал, что обе страны в целом согласуются, однако выявлен ряд различий. В 2025 году, введение ст. 274^5 УК РФ криминализировавший оборот средств доступа, приблизилось к имплементации положения ст. 11 Конвенция ООН

против киберпреступности. Иную картину, демонстрирует уголовное законодательство Кыргызской Республики в части криминализации оборота паролей, реквизитов доступа и электронных подписей, что свидетельствует о существующем пробеле и скорейшем законодательном восполнении. Кроме этого, странам рекомендуется закрепить оговорку, исключающую ответственность за легитимные действия специалистов по кибербезопасности, а также расширить объективную сторону ст. 273 УК РФ и ст. 320 УК КР, включив такие действия, как приобретения и (или) хранения вредоносных компьютерных программ (программных продуктов) в целях совершения иного преступления.

В ходе сравнительно-правового анализа, выявлены общие подходы и национальные особенности конструкций составов, связанных с вредоносными компьютерных программам, предусмотренные нормами уголовного законодательства стран СНГ. Особое внимание заслуживает УК Армении, в котором предусмотрено наличие специального основания для освобождения от уголовной ответственности в случае добровольной сдачи таких средств правоохранительным органам. Позитивным примером служит криминализация приобретения и (или) хранения в УК Азребайджана, Армении и Молдовы. Формальная конструкция составов принятая в большинстве стран СНГ является более эффективной, чем формально-материальная конструкция основного состава в УК Кыргызстана, требующая наступления значительного ущерба для привлечения к ответственности за использование или распространение вредоносного программного продукта.

Детальный анализ признаков составов преступлений, предусмотренных ст. 273 УК РФ и ст. 320 УК КР, позволил выявить их существенные доктринальные и законодательные различия.

Ключевым отличием является предмет преступления: ст. 273 УК РФ, который содержит, такие понятия как «вредоносная компьютерная программа» и «иная вредоносная компьютерная информация», в то время как ст. 320 УК КР ограничивается только «программным продуктом». Кроме этого, отсутствие в ст. 273 УК РФ такого действия, как «внесение изменений в существующие

программы», которое было исключено российским законодателем в 2011 г., но присутствует в ст. 320 УК КР.

Другим существенными отличиями являются: конструкция состава: в России основной состав ст. 273 УК РФ является формальным, а в Кыргызстане состав является формально-материальным, который требует для квалификации использования или распространения программного продукта наступления значительного ущерба. В ст. 273 УК РФ цель является факультативным признаком, в то время как в ст. 320 УК КР создание в целях использования или распространение является обязательным признаком состава.

На основе проведенного исследования сформулированы следующие основные предложения по совершенствованию уголовного законодательства Российской Федерации и Кыргызской Республики.

В отношении уголовного законодательства Российской Федерации предлагается: вернуть ранее исключенное действие «внесение изменений в существующие программы», расширить объективную сторону ст. 273 УК РФ, дополнив диспозицию такими действиями, как «приобретение» и (или) «хранение» вредоносных компьютерных программ или иной вредоносной компьютерной информации в целях совершения иного преступления; ввести оговорку о неприменении статьи в отношении действий, совершенных в разрешенных целях тестирования, исследования или защиты информационных систем, что будет консолидироваться с п. 2 ст. 11 Конвенции ООН против киберпреступности.

В отношении уголовного законодательства Кыргызской Республики предлагается следующее: расширить предмет преступления, предусмотренного ст. 320 УК КР, включив в него наряду с «программным продуктом» также «иную вредоносную компьютерную информацию»; в ч. 2 ст. 320 УК КР; изменить конструкцию основного состава преступления, исключив из ч. 1 ст. 320 УК КР указание на обязательное наступление «значительного ущерба» в качестве условия ответственности за использование и распространение вредоносных программных продуктов, сделав состав формальным; дополнить ст. 320 УК КР примечанием, закрепляющим определение вредоносного программного продукта.

Актуальным вопросом для обеих стран является возможный переход в уголовном законодательстве к использованию более широких и современных понятий, таких как как «цифровая вредоносная программа» и «цифровая информация».

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

Международные нормативно-правовые акты:

1. Конвенция Организации Объединенных Наций против киберпреступности; укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям, 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 (дата обращения: 20.02.2026).

2. Конвенция о преступности в сфере компьютерной информации от 23 ноября 2001 г. ETS № 185 // ЭПС «Система ГАРАНТ». [Электронный ресурс]. – URL: http://base.garant.ru/4089723 (дата обращения: 09.01.2025).

3. Соглашение о сотрудничестве государств в борьбе с преступлениями в сфере компьютерной информации от 1 июня 2001 г. // Законодательство стран СНГ. – URL: https://base.garant.ru/12123778/ (дата обращения: 21.03.2025).

4. Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий 2018 г. // Законодательство стран СНГ. – URL: https://base.spinform.ru/show_doc.fwx?rgn=110821 (дата обращения: 13.02.2025).

5. Соглашение между правительствами государств – членов ШОС о сотрудничестве в области обеспечения информационной безопасности 2009 г. // Официальный сайт ШОС. – URL: https://ccdcoe.org/sites/default/files/documents/SCO-090616IISAgreementRussian (дата обращения: 13.02.2025).

6. Конвенция Лиги арабских государств о борьбе с преступлениями в сфере информационных технологий 2010 г. – URL: https://www.asianlaws.org/gcld/cyberlawdb/GCC/Arab%20Convention%20on%20Com

bating%20Information%20Technology%200ffences.pdf. (дата обращения: 13.02.2025).

7. Конвенция Африканского союза о кибербезопасности и защите персональных данных 2014 г. // Официальный сайт Африканского союза. – URL: https://au.int/en/treaties/african-union-convention-cyber-security-and personal-data-protection (дата обращения: 21.02.2025).

8. Второй Дополнительный протокол к Будапештской конвенции 2001 г. – URL: https://www.coe.int/en/web/deputy-secretary-general/-/treaty-signature-ceremony-of-the-second-additional-protocol-to-the-convention-on-cybercrime-on-enhanced-co-operation-and-disclosure-of-electronic-evid (дата обращения: 15.03.2025).

9. Резолюция Генеральной Ассамблеи ООН A/RES/74/247 от 27 декабря 2019 г. «Противодействие использованию информационно-коммуникационных технологий в преступных целях» // Официальный сайт ООН. – URL: https://docs.un.org/ru/A/RES/74/247 (дата обращения: 15.03.2025).

10. Резолюция Генеральной Ассамблеи ООН A/RES/75/282 от 26 мая 2021 г. «Противодействие использованию информационно-коммуникационных технологий в преступных целях» // Официальный сайт ООН. – URL: https://docs.un.org/ru/A/RES/75/282 (дата обращения: 15.03.2025).

11. Резолюция Генеральной Ассамблеи ООН A/RES/79/243 от 24 декабря 2024 г. «Противодействие использованию информационно-коммуникационных технологий в преступных целях» // Официальный сайт ООН. – URL: https://docs.un.org/ru/A/RES/79/243 (дата обращения: 15.03.2025).

Нормативно-правовые акты:

12. Конституция Российской Федерации: принята всенародным голосованием 12 декабря 1993 г.: с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 г. // Официальный интернет-портал правовой информации. – URL: http://www.pravo.gov.ru (дата обращения: 25.02.2026).

13. Закон Кыргызской Республики от 5 мая 2021 г. № 59 «О Конституции Кыргызской Республики» // Газета «Эркин-Тоо». – 2021. – 7 мая. – № 64. – URL: https://cbd.minjust.gov.kg/1-2/edition/1202952/ru (дата обращения: 25.02.2026).

14. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 20 февраля 2026 г.) // СЗ РФ. – 1996. – № 25. – Ст. 2954.

15. Уголовный кодекс Кыргызской Республики от 28 октября 2021 г. № 127 (по сост. на 1 января 2026 г.) [Электронный ресурс]. – URL: https://cbd.minjust.gov.kg/3-38/edition/2087/ru (дата обращения: 15.05.2025).

16. Уголовный кодекс Кыргызской Республики от 1 октября 1997 г. № 68 (утратил силу с 1 января 2019 г. в соответствии с Законом Кыргызской Республики от 24 января 2017 г. № 10) [Электронный ресурс]. – URL: https://cbd.minjust.gov.kg/3-10/edition/919984/ru (дата обращения: 15.05.2025).

17. Уголовный кодекс Кыргызской Республики от 2 февраля 2017 г. № 19 (утратил силу в соответствии с Законом КР от 28 октября 2021 г. № 126) [Электронный ресурс]. – URL: https://cbd.minjust.gov.kg/111527/edition/1186183/ru (дата обращения: 09.04.2025)

18. Кодекс Кыргызской Республики от 31 июля 2025 г. № 178 «Цифровой Кодекс Кыргызской Республики» [Электронный ресурс]. – URL: https://cbd.minjust.gov.kg/3-48/edition/35412/ru?lang=ru (дата обращения: 25.02.2025).

19. Федеральный закон от 7 декабря 2011 г. № 420-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» // СЗ РФ. – 2011. – № 50. – Ст. 7362.

20. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СЗ РФ. – 2006. – № 31 (ч. 1). – Ст. 3448.

21. Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» // СЗ РФ. – 1995. – № 33. – Ст. 3349.

22. Федеральный закон от 26 июля 2017 г. № 194-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-

процессуального кодекса Российской Федерации в связи с принятием Федерального закона “О безопасности критической информационной инфраструктуры Российской Федерации”» // СЗ РФ. – 2017. – № 31 (ч. 1). – Ст. 4743.

23. Федеральный закон от 30 ноября 2024 г. № 421-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» // СЗ РФ. – 2024. – № 49 (ч. 4). – Ст. 7412.

24. Федеральный закон от 31 июля 2025 г. № 282-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статьи 31 и 151 Уголовно-процессуального кодекса Российской Федерации» // Официальный интернет-портал правовой информации. – URL: http://publication.pravo.gov.ru/document/0001202507310013 (дата обращения: 20.12.2025).

25. Закон Кыргызской Республики от 3 марта 1998 г. № 28 «О правовой охране программ для электронных вычислительных машин и баз данных» // Газета «Эркин-Тоо». – 1998. – 4 апр. – № 28. – URL: https://cbd.minjust.gov.kg/39/edition/1240316/ru (дата обращения: 18.02.2025).

26. Закон Кыргызской Республики от 14 января 1998 г. № 6 «Об авторском праве и смежных правах» [Электронный ресурс]. – URL: https://cbd.minjust.gov.kg/17/edition/1240396/ru (дата обращения: 21.08.2025).

27. Закон Кыргызской Республики от 19 июля 2017 г. № 127 «Об электронном управлении» // Газета «Эркин-Тоо». – 2017. – 25 июля. – № 127. – URL: https://cbd.minjust.gov.kg/111634/edition/36815/ru (дата обращения: 15.02.2026).

28. Закон Кыргызской Республики от 26 июня 2025 г. № 127 «Об оперативно-розыскной деятельности» // Газета «Эркин-Тоо». –2025. –1 июля. – № 141. – URL: https://cbd.minjust.gov.kg/4-5574/edition/34556/ru (дата обращения: 20.02.2026).

29. Закон Кыргызской Республики от 2 апреля 1998 г. № 31 «Об электрической связи» // Газета Ведомости Жогорку Кенеша Кыргызской

Республики. – 1998. – № 8. – Ст. 230а. – URL: https://cbd.minjust.gov.kg/4-31/edition/36653/ru?lang=ru (дата обращения: 15.02.2026).

30. Закон Кыргызской Республики от 21 января 2020 г. № 14 «О ратификации Соглашения о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий, подписанного 28 сентября 2018 года в городе Душанбе» // Газета «Эркин Тоо». – 2020. – 24 янв. – № 7 (3079). – URL: https://cbd.minjust.gov.kg/4-2809/edition/992067/ru (дата обращения: 13.02.2025).

31. Закон Кыргызской Республики от 17 марта 2023 г. № 62 «О внесении изменений в Закон Кыргызской Республики "Об авторском праве и смежных правах" и признании утратившими силу некоторых законодательных актов Кыргызской Республики» // Газета «Эркин-Тоо». – 2023. – 24 марта. – № 62. – URL: https://cbd.minjust.gov.kg/112543/edition/1240272/ru (дата обращения: 18.02.2025).

32. Закон Кыргызской Республики от 14 апреля 2008 г. № 58 «Об информации персонального характера» // Газета «Эркин-Тоо». – 2008. – 18 апр. – № 4029. – URL: https://cbd.minjust.gov.kg/4-3703/edition/1239270/ru (дата обращения: 20.02.2026).

33. Закон Кыргызской Республики от 19 июля 2017 г. № 128 «Об электронной подписи» // Газета «Эркин-Тоо». – 2017. – 25 июля. – № 128. – URL: https://cbd.minjust.gov.kg/4-2446/edition/985628/ru (дата обращения: 20.02.2026).

34. Закон Кыргызской Республики от 31 июля 2025 г. № 179 «О введении в действие Цифрового кодекса Кыргызской Республики» // Газета «Эркин-Тоо». – 2025. – 5 авг. – № 195. – URL: https://cbd.minjust.gov.kg/4-5604/edition/35394/ru (дата обращения: 20.02.2026).

35. Закон Кыргызской Республики от 17 июля 2024 г. № 121 «О кибербезопасности Кыргызской Республики» // Газета «Эркин-Тоо». – 2024. – 19 июля. – № 123. – URL: https://cbd.minjust.gov.kg/4-5371/edition/13381/ru (дата обращения: 15.10.2025).

36. Уголовный кодекс Республики Казахстан от 3 июля 2014 г. № 226-V. (по сост. на 2 мая 2025 г.) [Электронный ресурс]. – URL: https://online.zakon.kz/Document/?doc_id=31575252 (дата обращения: 10.05.2025).

37. Уголовный кодекс Республики Таджикистан от 21 мая 1998 г. № 574. (по сост. на 24 апреля 2025 г.) [Электронный ресурс]. – URL: https://continent-online.com/Document/?doc_id=30397325 (дата обращения: 01.05.2025).

38. Уголовный Кодекс Республики Беларусь от 19 июля 1999 г. № 275-З. (по сост. на 24 апреля 2025 г.) [Электронный ресурс]. – URL: https://online.zakon.kz/Document/?doc_id=30414984 (дата обращения: 01.05.2025).

39. Уголовный кодекс Республики Узбекистан (утвержден Законом Республики Узбекистан от 22 сентября 1994 г. № 2012-XII) (по сост. на 24 апреля 2025 г.) [Электронный ресурс]. – URL: https://online.zakon.kz/Document/?doc_id=30421110 (дата обращения: 01.05.2025).

40. Уголовный кодекс Азербайджанской Республики (утвержден Законом Азербайджанской Республики от 30 декабря 1999 г. № 787-IQ). (по сост. на 11 мая 2025 г.) [Электронный ресурс]. – URL: https://continent-online.com/Document/?doc_id=30420353 (дата обращения: 18.05.2025).

41. Уголовный кодекс Республики Армения от 27 мая 2021 г. № ЗР-199. (по сост. на 13 мая 2025 г.) [Электронный ресурс]. – URL: https://continent-online.com/Document/?doc_id=39571894 (дата обращения: 20.05.2025).

42. Уголовный кодекс Туркменистана от 12 июня 1997 г. № 222-I (по сост. на 17 мая 2025 г.) [Электронный ресурс]. – URL: https://continent-online.com/Document/?doc_id=31295286 (дата обращения: 25.05.2025).

43. Уголовный кодекс Республики Молдова от 18 апреля 2002 г. № 985-XV. (по сост. на 17 мая 2025 г.) [Электронный ресурс]. – URL: https://continent-online.com/Document/?doc_id=30394923 (дата обращения: 25.05.2025).

44. Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СЗ РФ. – 2016. – № 50. – Ст. 7074.

45. Указ Президента Кыргызской Республики от 5 апреля 2024 г. УП № 90 «Об утверждении Концепции цифровой трансформации Кыргызской Республики на 2024–2028 годы» // Газета «Эркин-Тоо». – 2024. – 12 апр. – № 90. – URL: https://cbd.minjust.gov.kg/5-10577/edition/6413/ru (дата обращения: 10.02.2025).

46. Указ Президента Кыргызской Республики от 20 декабря 2021 г. УП № 570 «О Концепции национальной безопасности Кыргызской Республики» [Электронный ресурс] – URL: https://cbd.minjust.gov.kg/5-9804/edition/1118040/ru (дата обращения: 19.08.2025).

47. Распоряжение Президента РФ от 22 марта 2008 г. № 144-рп «О признании утратившим силу распоряжения Президента Российской Федерации от 15 ноября 2005 г. № 557-рп “О подписании Конвенции о киберпреступности”» // СЗ РФ. – 2008. – № 13. – Ст. 1295. .

48. Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // СЗ РФ. – 2017. – № 20. – Ст. 2901.

49. Постановление Правительства Кыргызской Республики от 7 августа 2014 г. № 451 «Об утверждении Перечня видов специальных технических средств, предназначенных для негласного получения информации в процессе осуществления оперативно-розыскной и контрразведывательной деятельности, а также применяемых при производстве специальных следственных действий» // Газета «Эркин-Тоо». –2014. – 12 августа. – № 451. – URL: https://cbd.minjust.gov.kg/7-17460/edition/1249991/ru (дата обращения: 20.02.2026).

50. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. – М.: Стандартинформ, 2008.

Судебная практика

51. 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». – URL: https://www.consultant.ru/document/cons_doc_LAW_434573/ (дата обращения: 15.02.2026).

52. Постановление Пленума Верховного Суда РФ от 27 января 1999 г. № 1 «О судебной практике по делам об убийстве (ст. 105 УК РФ)» // СПС «КонсультантПлюс». – URL: https://www.consultant.ru/document/cons_doc_LAW_21893/ (дата обращения: 30.05.2026).

53. Кассационное определение СК по уголовным делам Первого кассационного суда общей юрисдикции от 16 мая 2024 г. по делу № 77-1910/2024 [Электронный ресурс]. – Доступ из СПС «Гарант».

54. Кассационное постановление Седьмого кассационного суда общей юрисдикции от 9 октября 2024 г. по делу № 7У-5887/2024 [77-3247/2024] [Электронный ресурс]. – Доступ из СПС «Гарант».

55. Постановление Первого кассационного суда общей юрисдикции от 19 апреля 2023 г. по делу № 7У-2934/2023 [77-1806/2023] [Электронный ресурс]. – Доступ из СПС «Гарант».

56. Апелляционное постановление Новосибирского областного суда от 5 сентября 2025 г. по делу № 22-3384/2025 [Электронный ресурс]. – Доступ из СПС «Гарант».

57. Апелляционное постановление Оренбургского областного суда от 17 ноября 2016 г. по делу № 22-4323/2016 [Электронный ресурс]. – Доступ из СПС «Гарант».

58. Апелляционное определение СК по уголовным делам Верховного Суда Республики Крым от 3 сентября 2024 г. по делу № 22-2322/2024 [Электронный ресурс]. – Доступ из СПС «Гарант».

59. Приговор Дзержинского районного суда города Волгограда Волгоградской области от 15 ноября 2018 г. по делу № 1-357/2018 [Электронный ресурс]. – Доступ из СПС «Гарант».

60. Приговор Прохладненского районного суда Кабардино-Балкарской Республики от 23 апреля 2025 г. по делу № 1-161/2025 [Электронный ресурс]. – Доступ из СПС «Гарант».

61. Приговор Бердского городского суда Новосибирской области от 10 ноября 2025 г. по делу № 1-225/2025 [Электронный ресурс]. – Доступ из СПС «Гарант».

62. Приговор Выксунского городского суда Нижегородской области от 27 мая 2024 г. по делу № 1-139/2024 [Электронный ресурс]. – Доступ из СПС «Гарант».

63. Приговор Нефтеюганского районного суда Ханты-Мансийского автономного округа-Югры от 22 апреля 2019 г. по делу № 1-187/2019 [Электронный ресурс]. – Доступ из СПС «Гарант».

64. Приговор Железнодорожного районного суда г. Новосибирска Новосибирской области от 23 мая 2025 г. по делу № 1-24/2025 [Электронный ресурс]. – Доступ из СПС «Гарант».

65. Приговор Химкинского городского суда Московской области от 11 сентября 2025 г. по делу № 1-639/2025 [Электронный ресурс]. – Доступ из СПС «Гарант».

66. Приговор Свердловского районного суда г. Костромы Костромской области от 12 ноября 2025 г. по делу № 1-364/2025 [Электронный ресурс]. – Доступ из СПС «Гарант».

67. Приговор Железнодорожного районного суда г. Красноярска Красноярского края от 6 ноября 2025 г. по делу № 1-312/2025 [Электронный ресурс]. – Доступ из СПС «Гарант».

68. Приговор Магаданского городского суда Магаданской области от 3 октября 2025 г. по делу № 1-500/2025 [Электронный ресурс]. – Доступ из СПС «Гарант».

69. Апелляционное определение СК по уголовным делам Московского городского суда от 1 марта 2021 г. по делу № 10-2228/2021 [Электронный ресурс]. – Доступ из СПС «Гарант».

70. Приговор Кузьминского районного суда г. Москвы от 23 ноября 2020 г. по делу № 1-584/2020 [Электронный ресурс]. – Доступ из СПС «Гарант».

71. Приговор Нижневартовского городского суда Ханты-Мансийского автономного округа – Югры от 27 августа 2025 г. по делу № 1-1231/2025 [Электронный ресурс]. – Доступ из СПС «Гарант».

72. Приговор Октябрьского районного суда г. Томска от 21 октября 2022 г. по делу 1-981/2022 [Электронный ресурс]. – Доступ из СПС «Гарант».

73. Приговор Центрального районного суда г. Читы от 3 июня 2025 г. по делу № 1-371/2025 [Электронный ресурс]. – Доступ из СПС «Гарант».

74. Приговор Киселевского городского суда Кемеровской области от 24 ноября 2025 г. по делу № 1-312/2025 [Электронный ресурс]. – Доступ из СПС «Гарант».

75. Приговор Бабушкинского районного суда г. Москвы от 13 октября 2015 г. по делу № 01-0656/2015 [Электронный ресурс]. – Доступ из СПС «Гарант».

76. Апелляционное определение Московского городского суда от 27 ноября 2015 г. по делу № 10-16199/2015 [Электронный ресурс]. – Доступ из СПС «Гарант».

77. Приговор Одинцовского городского суда Московской области от 31 октября 2025 г. по делу № 1-1023/2025 [Электронный ресурс]. – Доступ из СПС «Гарант».

78. Приговор Индустриального районного суда г. Барнаула Алтайского края от 6 октября 2025 г. по делу № 1-408/2025 [Электронный ресурс]. – Доступ из СПС «Гарант».

79. Приговор Верх-Исетского районного суда г. Екатеринбурга от 6 июля 2022 г. по делу № 1-382/2022 [Электронный ресурс]. – Доступ из СПС «Гарант».

Диссертации и авторефераты диссертаций:

80. Бегишев, И.Р. Понятие и виды преступлений в сфере обращения цифровой информации: дис. ... канд. юрид. наук: 12.00.08 / Бегишев Ильдар Рустамович. – Казань, 2017. – 204 с.

81. Дворецкий, М.Ю. Преступления в сфере компьютерной информации (уголовно-правовое исследование): дис ... канд. юрид. наук: 12.00.08. / Дворецкий Михаил Юрьевич. – Волгоград, 2001. – 193 с.

82. Евдокимов, К.Н. Противодействие компьютерной преступности: теория, законодательство, практика: дис. ... д-ра юрид. наук: 12.00.08 / Евдокимов Константин Николаевич. – М., 2021. – 557 с.

83. Ефремова, М.А. Уголовно-правовая охрана информационной безопасности: дис. ... д-ра юрид. наук: 12.00.08 / Ефремова Марина Александровна. – М., 2017. – 427 с.

84. Лихачев, Н.А. Уголовно-правовое противодействие преступлениям в сфере обеспечения информационной безопасности: законодательный, правоприменительный и доктринальный аспекты: дис. …канд. юрид. наук: 5.1.4 / Лихачев Никита Александрович. – Краснодар, 2024. – 237 с.

85. Максимов, В.Ю. Незаконное обращение с вредоносными программами для ЭВМ: Проблемы криминализации, дифференциации ответственности и индивидуализации наказания: дис. ... канд. юрид. наук: 12.00.08 / Максимов Владимир Юрьевич. – Краснодар, 1998. – 169 с.

86. Малыковцев, М.М. Уголовная ответственность за создание, использование и распространение вредоносных программ для ЭВМ: дис. ... канд. юрид. наук: 12.00.08 / Малыковцев Михаил Михайлович. – М., 2006. – 186 с.

87. Маслакова, Е.А. Незаконный оборот вредоносных компьютерных программ: уголовно-правовые и криминологические аспекты: дис. ... канд. юрид. наук: 12.00.08 / Маслакова Елена Александровна. – М., 2008. – 198 с.

88. Мысина, А.И. Международно-правовое регулирование сотрудничества государств по противодействию преступлениям в сфере информационных технологий: дис. ...канд. юрид. наук. 12.00.10 / Мысина Анастасия Ильинична. – М., 2021. – 191 с.

89. Пучков, Д.В. Уголовно-правовая модель защиты телекоммуникаций от преступных посягательств: проблемы теории и практики: дис. ... д-ра. юрид. наук: 5.1.4 / Пучков Денис Валентинович. – Екатеринбург, 2022. – 474 с.

90. Русскевич, Е.А. Дифференциация ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий, и проблемы их квалификации: дис. ... д-ра юрид. наук: 12.00.08 / Русскевич Евгений Александрович. – М., 2020. – 521 с.

91. Степанов-Егиянц, В.Г. Методологическое и законодательное обеспечение безопасности компьютерной информации в Российской Федерации: уголовно-правовой аспект: дис. ... д-ра юрид. наук: 12.00.08 / Степанов-Егиянц Владимир Георгиевич. – М., 2016. – 389 с.

92. Тропина, Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дис. ... канд. юрид. наук: 12.00.08 / Тропина Татьяна Львовна. – Владивосток, 2005. – 235 с.

93. Усов, Е.Г. Уголовная ответственность за незаконный оборот специальных технических средств, предназначенных для негласного получения информации: дис. ... канд. юрид. наук: 12.00.08 / Усов Евгений Геннадьевич. – Иркутск, 2020. – 193 с.

Учебная литература:

94. Абдулвалиев, А.Ф. Уголовное право: Общая часть: учебник / А.Ф. Абдулвалиев [и др.]; под науч. ред. д-ра юрид. наук, проф. А. В. Сумачева, д-ра юрид. наук, проф. Р. Д. Шарапова; отв. ред. канд. юрид. наук, доц. Л. В. Иванова, канд. юрид. наук, доц. В. И. Морозов. – М.: ИНФРА-М, 2025. – 721 с.

95. Андрианов, В.К. Комментарий к Уголовному кодексу Российской Федерации (постатейный): в 2 т. / В.К. Андрианов, А. В. Бриллиантов, М. А. Кауфман и др. ; под ред. А. В. Бриллиантова. 3-е изд., перераб. и доп. – М.: Проспект, 2021. – 792 с.

96. Андрианов, В.К. Уголовное право России. Части Общая и Особенная: учебник / В.К. Андрианов, А.А. Арямов, В. А. Блинников и др.; под ред. А. В. Бриллиантова. – 3-е изд., перераб. и доп. – М.: Проспект, 2021. – 1344 с.

97. Арзамасцев, М.И. Уголовное право России: общая часть: учебник / М. И. Арзамасцев, А.И. Бойцов, В. Н. Бурлаков [и др.]; под ред. В.В. Лукьянова, В. С.

Прохорова, В. Ф. Щепелькова, – перераб. и доп. – СПб.: Издательство СПбГУ, 2013.– 600 с.

98. Асаналиев, Т.А. Комментарий к Уголовному кодексу (постатейный). Преступления и наказания в Кыргызской Республике / Т.А. Асаналиев, К. М. Осмоналиев. – Бишкек: Академия, 2004. – 710 с.

99. Барышева, К.А. Российское уголовное право. Особенная часть: учебник / К.А. Барышева, Ю.В. Грачева, Р.О. Долотов и др. ; под ред. Г.А. Есакова. – М.: Проспект, 2021. – 608 с.

100. Бастрыкин, А.И. Уголовное право. Особенная часть: учебник для вузов / А. И. Бастрыкин, А. И. Чучаев; под общ. ред. А. И. Бастрыкина ; под науч. ред. А. И. Чучаева. – М.: Юрайт, 2025. – 468 с.

101. Бимбинов, А.А. Уголовное право Российской Федерации. Особенная часть: учебник / А.А. Бимбинов, С.А. Боженок, Ю. В. Грачева и др.; под ред. И.Э. Звечаровского. – М.: Проспект, 2020. – 688 с.

102. Боровиков, В.Б. Уголовное право. Особенная часть: учебник для вузов / В.Б. Боровиков, А.А. Смердов; под ред. В.Б. Боровикова. – 7-е изд., перераб. и доп. – М. : Юрайт, 2025. – 479 с.

103. Голик, Ю.В. Уголовно-правовая политика. Тенденции и перспективы / Ю.В. Голик, А.И. Коробеев, А. В. Усс. – Красноярск: Изд-во Краснояр. ун-та, 1991. – 240 с.

104. Грачева, Ю.В. Риски цифровизации. Виды, характеристика, уголовно-правовая оценка: монография / Ю.В. Грачева, С.А. Иванов, С.В. Маликов, А.И. Чучаев; отв. ред. д-р юрид. наук, проф. Ю.В. Грачева. – М.: Проспект, 2022. – 272 с.

105. Грачева, Ю. В. Уголовное право России. Общая и особенная части: учебник / Ю. В. Грачева, А. И. Чучаев. – М.: Контракт, НИЦ ИНФРА-М, 2017. – 384 с.

106. Дворецкий, М.Ю. Преступления в сфере компьютерной информации: понятие, система, проблемы квалификации и наказания : Монография / М.Ю.

Дворецкий; – М-во образования Рос. Федерации. Тамб. гос. ун-т им. Г.Р. Державина. – Тамбов : Изд-во ТГУ, – 2003. – 197 с.

107. Дворянсков, И.В. Уголовное право. Особенная часть: учебник / И. В. Дворянсков; под ред. д-ра юрид. наук, проф. И.В. Дворянскова. – М.: ИНФРА-М, 2025. – 583 с.

108. Дремлюга, Р.И. Уголовно-правовая охрана цифровой экономики и информационного общества от киберпреступных посягательств: доктрина, закон, правоприменение: монография / Р. И. Дремлюга. – М. : Юрлитинформ, 2022. – 325 с.

109. Евдокимов, К.Н. Создание, использование и распространение вредоносных компьютерных программ: уголовно-правовые и криминологические аспекты: монография / К.Н. Евдокимов. – Иркутск : Иркутский юридический институт (филиал) Академии Генеральной прокуратуры РФ, 2013. – 267 с.

110. Ефремова, И.А. Уголовное право (Особенная часть): курс лекций / И.А. Ефремова; под ред. и с предисл. Б.Т. Разгильдиева; Саратовская государственная юридическая академия. – Саратов: Изд-во Сарат. гос. юрид. акад., 2023. – 465 с.

111. Ефремова, М.А. Уголовная ответственность за преступления, совершаемые с использованием информационно-телекоммуникационных технологий / М.А. Ефремова. – М. : Юрлитинформ, 2015. - 194, [1] с.; 22 см. – (Уголовное право).; ISBN 978-5-4396-0774-7.

112. Иногамова-Хегай, Л.В. Уголовное право Российской Федерации. Общая часть: учебник / Л. В. Иногамова-Хегай; под ред. д-ра юрид. наук, проф. Л. В. Иногамовой-Хегай. – 3-е изд., перераб. и доп. – М.: ИНФРА-М, 2022. – 354 с.

113. Калиниченко, И.А. Противодействие преступлениям в сфере информационных технологий: учебник / И.А. Калиниченко, А.В. Андреев, Д.В. Галиев [и др.]; под науч. ред. И.А. Калиниченко; под техн. ред. В.В. Гончара. – М.: ИНФРА-М, 2025. – 862 с.

114. Козаев, Н.Ш. Современные технологии и проблемы уголовного права (анализ зарубежного и российского законодательства): монография / Н.Ш. Козаев; под ред. А.В. Наумова. – М. : Юрлитинформ, 2015. – 217, [1] с.; 22 см.

115. Козаченко, И.Я. Уголовное право. Особенная часть: учебник / И. Я. Козаченко, Г. П. Новоселов; отв. ред. И. Я. Козаченко, Г. П. Новоселов. – 5-е изд., изм. и доп. – М.: Норма: НИЦ ИНФРА-М, 2013. – 912 с.

116. Корабельников, С. М. Преступления в сфере информационной безопасности: учеб. пособие для вузов / С. М. Корабельников. – М.: Юрайт, 2024. – 111 с.

117. Курманов, К.Ш. Уголовное право Кыргызской Республики (Особенная часть) / К. Ш. Курманов; под ред. и с предисл. К. Ш. Курманова. – Бишкек : Наука и образование, 2001. – 620 с.

118. Лебедев, В. М. Комментарий к Уголовному кодексу РФ: в 4 т. Т. 3. Особенная часть. Раздел IX / В. М. Лебедев; отв. ред. В. М. Лебедев. –М.: Юрайт, 2026. – 296 с.

119. Лопашенко, Н.А. Уголовная политика / Н.А. Лопашенко. – М.: Волтерс Клувер, 2009. – 579 с.

120. Наумов, А.В., Кибальник А.Г. Преступления против общественной безопасности и общественного порядка : учебник для вузов / А. В. Наумов, А. Г. Кибальник; отв. ред. А. В. Наумов, А. Г. Кибальник. – 6-е изд., перераб. и доп. – М.: Юрайт, 2025. – 168 с.

121. Осмоналиев, К.М. Уголовное право Кыргызской Республики (Особенная часть): учеб. пособие / К. М. Осмоналиев; под общ. ред. проф. В. П. Ревина. – 2-е изд. – Бишкек: Раритет Инфо, 2005. – 321 с.

122. Российское уголовное право. Общая часть: учебник / под ред. В. П. Коняхина. – М.: Контракт, НИЦ ИНФРА-М, 2016. – 560 с.

123. Русскевич, Е.А. Компьютерные преступления: квалификационные алгоритмы и тренды: учебное пособие / Е. А. Русскевич. – М.: Проспект, 2025. – 120 с.

124. Русскевич, Е.А. Уголовное право и «цифровая преступность»: проблемы и решения: монография / Е.А. Русскевич. – 2-е изд., перераб. и доп. – М. : ИНФРА-М, 2023. – 351 с.

125. Сверчков, В.В. Уголовное право. Особенная часть: учебник для вузов / В.В. Сверчков. – 12-е изд., перераб. и доп. – М.: Юрайт, 2025.– 421 с.

126. Сыдыкова, Л.Ч. Уголовное право Кыргызской Республики. Общая часть. Преступление. Наказание: учебник / Л.Ч. Сыдыкова. – Бишкек : Издательский дом КРСУ, 2023. – 253 с.

127. Уголовное право России. Особенная часть: учебник / под ред. В.Н. Бурлакова, В.В. Векленко, В.Ф. Щепелькова. – 4-е изд., доп. – СПб : СПбГУ, 2022. – 896 с.

128. Уголовное право России. Части Общая и Особенная: учебник для бакалавров / отв. ред. А.И. Рарог. – 2-е изд., перераб. и доп. – М.: Проспект, 2020. – 624 с.

129. Уголовное право Российской Федерации. Особенная часть: учебник / под ред. проф. Л.В. Иногамовой-Хегай. – 3-е изд., перераб. и доп. –М.: ИНФРА-М, 2026. – 407 с.

130. Уголовное право. Особенная часть : учебник для вузов / отв. ред. А.В. Наумов, А.Г. Кибальник. – 6-е изд., перераб. и доп. – М.: Юрайт, 2025. – 564 с.

131. Уголовное право. Особенная часть: учебник для бакалавров / под ред. А. И. Чучаева. – 3-е изд., перераб. и доп. – М.: Проспект, 2018. – 462 с.

Научные статьи:

132. Архипова, Е.А. Международно-правовые проблемы сотрудничества при выявлении, расследовании и предупреждении преступлений, совершенных с использованием информационно-телекоммуникационных сетей и в сфере компьютерной информации / Е. А. Архипова, В. Н. Додонов // Московский журнал международного права. – 2020. – № 2. – С. 77–87.

133. Атабеков, К.К. Новое уголовное законодательство Кыргызской Республики: предпосылки принятия и некоторые его коллизии / К. К. Атабеков // Экономика. Право. Общество. – 2024. – Т. 9. – № 1. – С. 83–86.

134. Вехов, В.Б. Вредоносные компьютерные программы как предмет и средство совершения преступления / В.Б. Вехов // Расследование преступлений: проблемы и пути их решения. – 2015. – № 2 (8). – С. 43–46.

135. Вострова, А.Н. Развитие уголовного законодательства Кыргызской Республики об ответственности за киберпреступления / А.Н. Вострова // Расследование преступлений: проблемы и пути их решения. – 2025. – № 2. – С. 142–146.

136. Голобородько, И. Л. Преступления в компьютерной сфере / И.Л. Голобородько // Научные исследования в Кыргызской Республике. – 2025. – № 2. – С. 107–114.

137. Дворецкий, М.Ю. Корреляции главы 28 УК РФ в контексте оптимизации уголовной ответственности и повышения эффективности правоприменительной практики / М. Ю. Дворецкий // Вестник ТГУ. – 2012. – № 6. – С. 266–271.

138. Дремлюга, Р.И. Преступления в виртуальной реальности: миф или реальность? / Р.И. Дремлюга, А.В. Крипакова // Актуальные проблемы российского права. – 2019. – № 3. – С. 161–169.

139. Дремлюга, Р.И. Уголовно-правовая политика в сфере противодействия платформизации преступной деятельности / Р. И. Дремлюга, А. И. Коробеев // Всероссийский криминологический журнал. – 2022. – Т. 16. – № 1. – С. 47–56.

140. Дремлюга Р.И., Зотов С.С., Павлинская В.Ю. Критическая информационная инфраструктура как предмет преступного посягательства // Азиатско-Тихоокеанский регион: экономика, политика, право. – 2019. – Т. 21. – № 2. – С. 130-139.

141. Дробот, Е.В. Новые приоритеты национальной безопасности стран Африки в условиях нарушения глобальных цепочек создания стоимости / Е. В. Дробот // Экономические отношения. – 2022. – Т. 12. – № 2. – С. 285–308.

142. Евдокимов, К.Н. К вопросу об объекте преступления при создании, использовании и распространении вредоносных программ для ЭВМ (ст. 273 УК

РФ) / К. Н. Евдокимов // Сибирский юридический вестник. – 2009. – № 4. – С. 39–44.

143. Евдокимов, К.Н. Принципы противодействия технотронной преступности: онтологические и гносеологические аспекты / К. Н. Евдокимов // Российская юстиция. – 2020. – № 3. – С. 56–58.

144. Ермолович, Я.Н. Научно-практический комментарий к Федеральному закону «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации» от 14 июля 2022 года № 260-ФЗ / Я.Н. Ермолович // Право в Вооруженных Силах. – 2022. – № 11. – С. 89–102.

145. Захарян, С.Ю. Основания криминализации и социальная обусловленность организации деятельности по передаче абонентских номеров с нарушением требований законодательства Российской Федерации / С.Ю. Захарян // Проблемы права. – 2025. – № 4 (100). – С. 108–118.

146. Кириленко, В.П. Гармонизация российского уголовного законодательства о противодействии киберпреступности с правовыми стандартами Совета Европы / В.П. Кириленко, Г.В. Алексеев // Всероссийский криминологический журнал. – 2020. – № 14 (6). – С. 898–913.

147. Корпеев, А.Г. Об объекте преступлений, совершаемых с использованием информационно-телекоммуникационных сетей, по уголовному законодательству России и Туркменистана / А.Г. Корпеев // Юридический аналитический журнал. – 2022. – Т. 17. – № 1. – С. 29–33.

148. Кравчук, С.В. К вопросу о социальной обусловленности криминализации незаконного использования абонентского терминала пропуска трафика или виртуальной телефонной станции / С.В. Кравчук // Проблемы права. – 2025. – № 4 (100). – С. 129–138.

149. Маслакова, Е.А. Анализ объективной стороны преступления, связанного с незаконным оборотом вредоносных компьютерных программ / Е.А. Маслакова // Известия ТулГУ. Экономические и юридические науки. – 2008. – № 1. – С. 225–232.

150. Мороз, Н.О. Актуальные вопросы международного сотрудничества в борьбе с преступностью в сфере высоких технологий в рамках СНГ / Н.О. Мороз // Международное уголовное право и международная юстиция. – 2016. – № 3. – С. 12–14.

151. Муратшина, К.Г. К вопросу о сотрудничестве в области информационной безопасности в рамках БРИКС / К.Г. Муратшина // Гуманитарное знание и искусственный интеллект: стратегии и инновации: 4-й молодежный конвент УрФУ: материалы международной конференции 26 марта 2020 года. – Екатеринбург: Изд во Урал. ун та. – 2020. – С. 614–621.

152. Поляков, В.В. Формирование экосистем преступных сообществ как следствие цифровой трансформации организованной преступной деятельности / В.В. Поляков // Вестник Томского государственного университета. – 2025. – № 511. – С. 229–236.

153. Пучков, Д.В. Глобальная политика в сфере уголовно-правовой защиты общества от киберпреступности: международные обязательства Российской Федерации при ратификации Конвенции ООН (2024) / Д.В. Пучков // Правопорядок: история, теория, практика. – 2025. – № 3 (46). – С. 147–153.

154. Русскевич, Е.А. Понятие вредоносной компьютерной программы / Е.А. Русскевич // Актуальные проблемы российского права. – 2018. – № 11. – С. 207–215.

155. Саркисян, А.Ж. Транснациональный характер преступности в киберпространстве / А.Ж. Саркисян // Расследование преступлений: проблемы и пути их решения. – 2024. – № 3. – С. 71–75.

156. Сейдакматов, Н. А. Правовое обеспечение информационной безопасности / Н. А. Сейдакматов // Вестник КРСУ. – 2024. – Т. 24. – № 3. – С. 101–106.

157. Сыдыкова, Л. Ч. Проблемы и пути развития современной уголовной политики в Кыргызстане / Л. Ч. Сыдыкова // Вестник КРСУ. – 2025. – Т. 25. – № 11. – С. 113–120.

158. Фомина, Л.Ю. Международные стандарты защиты персональных данных в условиях информационного общества / Л.Ю. Фомина // Международное право. – 2019. – № 4. – С. 50–59.

159. Шестак, В.А., Чеботарь А.С. Будапештская конвенция как основополагающий механизм противодействия киберпреступности: новации и перспективы международно-правового регулирования / В.А. Шестак, А. С. Чеботарь // Образование и право. – 2023. – № 8. – С. 305–310.

160. Щепельков, В.Ф. Перспективы уголовно-правового противодействия компьютерным преступлениям / В.Ф. Щепельков // Вестник Волгоградской академии МВД России. – 2024. – № 3 (70). – С. 9–14.

161. Энгельгардт, А. А. Компьютерная информация как предмет преступления, предусмотренного статьей 273 Уголовного кодекса Российской Федерации / А.А. Энгельгардт // Право. Журнал Высшей школы экономики. – 2014. – № 4. – С. 136–145.

162. Яни, П.С. Проблемы квалификации преступлений в сфере гособоронзаказа / П.С. Яни // Законность. – 2023. – № 9. – С. 44–49.

Интернет – ресурсы:

163. Collins, S. Stuxnet: the emergence of a new cyber weapon and its implications / S. Collins, S. McCombie // Journal of Policing, Intelligence and Counter Terrorism. – 2012. – Vol. 7(1). – P. 80–91. – URL: https://doi.org/10.1080/18335330.2012.65319.

164. Состояние преступности в Российской Федерации за январь – декабрь 2021 год. [Электронный ресурс]. – URL: https://xn--b1aew.xn--p1ai/reports/item/28021552/ (дата обращения: 25.02.2026).

165. Состояние преступности в Российской Федерации за январь – декабрь 2022 год. [Электронный ресурс]. – URL: https://xn--b1aew.xn--p1ai/reports/item/35396677/ (дата обращения: 25.02.2026).

166. Состояние преступности в Российской Федерации за январь – декабрь 2023 год. [Электронный ресурс]. – URL: https://xn--b1aew.xn--p1ai/reports/item/47055751/ (дата обращения: 25.02.2026).

167. Состояние преступности в Российской Федерации за январь – декабрь 2024 год. [Электронный ресурс]. – URL: https://xn--b1aew.xn--p1ai/reports/item/60248328/ (дата обращения: 25.02.2026).

168. Состояние преступности в Российской Федерации за январь – декабрь 2025 год. [Электронный ресурс]. – URL: https://xn--b1aew.xn--p1ai/reports/item/77848182/ (дата обращения: 25.02.2026).

169. NotPetya: червь на десять миллиардов долларов. – URL: https://www.dna.fi/dnabusiness/blogi/-/blogs/notpetya-the-ten-billion-dollar-worm (дата обращения: 05.01.2026).

170. Philip Elmer-Dewitt (26 сентября 1988). – URL: https://time.com/archive/6713325/technology-you-must-be-punished/ (дата обращения: 09.01.2025).

171. Автор оригинального вируса-вымогателя Petya опубликовал главный ключ расшифровки. – URL: https://www.bleepingcomputer.com/news/security/author-of-original-petya-ransomware-publishes-master-decryption-key/ (дата обращения: 05.01.2026).

172. В Кыргызстане каждый тридцатый компьютер атакуют вредоносные программы. – URL: https://rg.ru/2025/06/04/v-kyrgyzstane-kazhdyj-tridcatyj-kompiuter-atakuiut-vredonosnye-programmy.html?ysclid=mnd9ulpmbs703845578&utm_referrer=https%3A%2F%2Fyandex.ru%2F (дата обращения: 13.04.2026).

173. В России вынесли первый приговор за продажу читов для World of Tanks. – URL: https://www.rbc.ru/rbcfreenews/62c5cbae9a794702dc6c2b6f (дата обращения: 15.04.2026).

174. Взлом с использованием ИИ: типы киберпреступлений с использованием ИИ и способы обезопасить себя – URL:

https://www.kaspersky.ru/resource-center/preemptive-safety/ai-cybercrime (дата обращения: 12.06.2026).

175. Даркнет (теневой интернет, DarkNet). – URL: https://www.tadviser.ru/index.php/,_DarkNet (дата обращения: 05.03.2026).

176. Доклад Генерального секретаря ООН от 30 июля 2019 г. в соответствии с Резолюцией Генеральной Ассамблеи ООН A/RES/73/187 от 17 декабря 2018 г., озаглавленной «Противодействие использованию информационно-коммуникационных технологий в преступных целях» // Официальный сайт ООН. URL: Официальный сайт ООН. – URL: https://docs.un.org/ru/A/74/130 (дата обращения: 15.03.2025).

177. Кыргызстан и Будапештская конвенция: цифровая безопасность как вызов времени. – URL: https://mnenie.akipress.org/unews/un_post:44659/ (дата обращения: 14.04.2026).

178. Материалы IX Конгресса ООН по предупреждению преступности и обращению с правонарушителями. – URL: http: www.un.org (дата обращения: 09.01.2025).

179. Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации. – М.: Генеральная Прокуратура РФ, 2013. – URL: https://epp.genproc.gov.ru/web/gprf/documents (дата обращения: 08.09.2025).

180. Новое уголовное законодательство Кыргызстана: откат назад или курс на результативность? – URL: https://cabar.asia/ru/novoe-ugolovnoe-zakonodatelstvo-kyrgyzstana-otkat-nazad-ili-kurs-na-rezultativnost (дата обращения: 25.12.2025).

181. Открытие Центра по обеспечению кибербезопасности [Электронный ресурс]. – URL: https://ru.sputnik.kg/20230513/kyrgyzstan-kiberbezopasnost-zdanie-centr-gknb-1075288960.html (дата обращения: 10.02.2026).

182. См.: Статистические данные по уголовным делам, рассмотренным судами первой инстанции за 9 месяцев 2025 года. [Электронный ресурс]. URL: https://sot.kg/statistics/main/index.php (дата обращения: 15.04.2026).

183. По следу хакеров. – URL: https://www.kommersant.ru/doc/4432198?ysclid=mnd9pny0hu401328144 (дата обращения: 11.04.2026).

184. Пояснительная записка к Проекту Постановления Правительства РФ «Об утверждении правил проверки соответствия пользователей государственной информационной системы, определенной в соответствии с частью 2 статьи 13.1 Федерального закона «О персональных данных», требованиям, указанным в части 7 статьи 13.1 Федерального закона «О персональных данных» о внесении изменений в некоторые акты Правительства Российской Федерации» (подготовлен Минцифры России, ID проекта 01/01/02-25/00154667) – URL: https://www.garant.ru/products/ipo/prime/doc/56914908/ (дата обращения: 10.02.2025).

185. Пояснительная записка к проекту федерального закона № 502113-8 «О внесении изменений в Уголовный кодекс Российской Федерации» (ред., внесенная в ГД ФС РФ, текст по состоянию на 4 декабря 2023 г.) // Государственная Дума Федерального Собрания Российской Федерации. – Система обеспечения законодательной деятельности (СОЗД). – URL: https://sozd.duma.gov.ru/bill/502113-8 (дата обращения: 10.05.2025).

186. Представляем HybridPetya: аналог Petya/NotPetya с обходом защиты UEFI Secure Boot. – URL: https://www.welivesecurity.com/en/eset-research/introducing-hybridpetya-petya-notpetya-copycat-uefi-secure-boot-bypass/ (дата обращения: 05.01.2026).

187. Принят план совместных действий стран БРИКС в области ИКТ // Министерство цифрового развития, связи и массовых коммуникаций РФ. – URL: https://digital.gov.ru/news/prinyat-plan-sovmestnyh-dejstvij-stran-briks-v-oblasti-ikt (дата обращения: 25.03.2025).

188. Сажать без штрафов и отменить Кодекс о проступках – проект нового УК КР. – URL: https://ru.sputnik.kg/20210510/kyrgyzstan-ugolovnyy-kodeks-izmeneniya-1052449627.html (дата обращения: 25.12.2025).

189. Сайт Налоговой службы Кыргызстана подвергся хакерской атаке. – URL: https://ru.sputnik.kg/20231019/sayt-nalogovoy-sluzhby-kyrgyzstana-podvergsya-khakerskoy-atake-1079673967.html (дата обращения: 11.04.2026).

190. Сборник актуальных документов Совета Министров внутренних дел. – М.: [б. и.], 2022. – № 3. – С. 90. – URL: https://mvd.gov.kg/media/gender_politic/%D0%A1%D0%B1%D0%BE%D1%80%D0%BD%D0%B8%D0%BA_%D1%80%D0%B5%D1%88%D0%B5%D0%BD%D0%B8%D0%B9_%D0%A1%D0%9C%D0%92%D0%94_2019-2022_3.pdf (дата обращения: 16.02.2026).

191. Справка-обоснование к проекту Цифрового кодекса Кыргызской Республики, № 6-6296/24, 18-06-2024. – URL: https://kenesh.kg/bills/653899 (дата обращения: 01.03.2025).

192. Статистические данные по уголовным делам, рассмотренным судами первой инстанции за 9 месяцев 2025 года. [Электронный ресурс]. – URL: https://sot.kg/statistics/main/index.php (дата обращения: 15.04.2026).

193. Хакеры «слили» в Сеть персональные данные 630 тысяч кыргызстанцев. – URL: https://economist.kg/novosti/2024/06/05/khakiery-slili-v-siet-piersonalnyie-dannyie 630tysiachkyrghyzstantsiev/?ysclid=mnd9xgnxq847623602 (дата обращения: 14.04.2026).

194. Шестьдесят пять стран подписали Конвенцию ООН против киберпреступности. – URL: https://news.un.org/ru/story/2025/10/1466671 (дата обращения: 25.12.2025).

195. Эксперты выявили вредоносное ПО Webrat для кражи данных геймеров и чит-кодов к играм. – URL: https://www.forbes.ru/tekhnologii/537866-eksperty-vyavili-vredonosnoe-po-webrat-dla-krazi-dannyh-gejmerov-i-cit-kodov-k-igram (дата обращения: 15.04.2026).

ПРИЛОЖЕНИЕ № 1

АНКЕТА

Уважаемые коллеги!

Прошу Вас принять участие в социологическом опросе, проводимом в рамках диссертационного исследования на тему: «Создание, использование и распространение вредоносных компьютерных программ по законодательству Российской Федерации и Кыргызской Республики: сравнительно-правовое исследование».

В анкетировании приняли участие **67 респондентов**.

Укажите Вашу профессиональную сферу деятельности:	
a) Научно-педагогическая деятельность (вуз, НИИ)	52,2%
b) Правоприменительная практика (судья, прокурор, следователь, адвокат и др.)	25,4%
c) Специалист в области информационной безопасности (включая аудит)	13,4%
d) Иное (укажите):	9%
Ваше гражданство (страна проживания)?	
a) Российской Федерации	61,5%
b) Кыргызской Республики	38,5%
c) Иное (укажите):	0%
Сталкивались ли Вы (или Ваши близкие/коллеги) с проблемой воздействия вредоносных компьютерных программ на территории Кыргызской Республики?	
a) Да, я лично подвергался атаке с использованием вредоносных программ	44,8%
b) Да, с такой проблемой сталкивались мои близкие/знакомые	23,9%

c) Да, в силу моей профессиональной деятельности мне известны случаи воздействия вредоносных программ (на предприятиях, у клиентов и т.п.)	11,9%
d) Нет, ни я, ни мое окружение с этим не сталкивались	10,4%
e) Затрудняюсь ответить / Не интересовался этим вопросом	9%
Насколько острой, по Вашему мнению, является проблема «правового вакуума» в отношении новых форм вредоносного программного обеспечения (скриптов, фрагментов кода, ключей доступа) в современном уголовном праве?	
a) Проблема крайне острая, законодательство не успевает за технологиями	65,1%
b) Проблема существует, но ее можно решить расширительным толкованием существующих норм	17,5%
c) Проблема надумана, действующих норм достаточно	14,3%
d) Затрудняюсь ответить	3,2%
Какие, на Ваш взгляд, основные препятствия существуют для эффективной уголовно-правовой борьбы с незаконным оборотом вредоносных программ в России и Кыргызстане?	
a) Несовершенство законодательства (терминология, составы преступлений)	28,8%
b) Высокая латентность и сложность выявления данных преступлений	27,1%
c) Отсутствие необходимых специальных знаний у следователей и судей	18,6%
d) Трансграничный характер киберпреступности и проблемы международного сотрудничества	16,9%
e) Отсутствие единой судебной практики и разъяснений высших судов	6,8%
f) Свой вариант:	1,7%

Согласны ли Вы с предложением расширить предмет ст. 320 УК Кыргызской Республики по модели ст. 273 УК РФ, включив в него «иную вредоносную компьютерную информацию»?	
a) Да, это предложение является своевременным и закроет существующие пробелы	53,3%
b) Скорее да, но потребуется четкое разъяснение термина	38,3%
c) Скорее нет, это может привести к излишней криминализации деяний	5%
d) Нет, существующего понятия «программный продукт» достаточно для квалификации	3,3%
Как Вы оцениваете термин «иная вредоносная компьютерная информация» (в контексте ст. 273 УК РФ и предложений по ст. 320 УК КР) с точки зрения юридической техники?	
a) Термин удачный, он позволяет гибко реагировать на технологические изменения	53,3%
b) Термин слишком оценочный, что создает риски злоупотреблений и требует конкретизации	30%
c) Термин требует замены на более точный, например «вредоносные цифровые объекты/данные»	10%
d) Затрудняюсь ответить	6,7%
Насколько обоснованным, по Вашему мнению, является предложение о возвращении в диспозицию ст. 273 УК РФ такого деяния, как «внесение изменений» в вредоносные программы?	
a) Предложение обосновано полностью, это устранит правовую неопределенность	40%
b) Предложение спорно, так как «внесение изменений» можно рассматривать как разновидность создания или модификации	36,7%
c) Предложение излишне, действующая редакция (создание, использование, распространение) охватывает все необходимые действия	15%

d) Затрудняюсь ответить	8,3%
Поддерживаете ли Вы криминализацию приобретения и (или) хранения вредоносных компьютерных программ или вредоносной информации?	
a) Да, поддерживаю в любом виде	41%
b) Да, но только при наличии цели совершения иного преступления (например, для последующего хищения денежных средств)	36,1%
c) Нет, не поддерживаю, так как это создает риск необоснованного привлечения к ответственности (например, для исследователей безопасности, коллекционеров, студентов)	18%
d) Затрудняюсь ответить	4,9%
Как Вы оцениваете уровень общественной опасности простого приобретения и хранения вредоносной компьютерной программы (без цели ее использования, распространения или совершения иного преступления)?	
a) Высокий уровень опасности (само по себе хранение таких объектов должно быть уголовно наказуемо)	40%
b) Средний уровень опасности	35%
c) Низкий уровень опасности	15%
d) Отсутствие общественной опасности (деяние является нейтральным)	10%
Как Вы оцениваете предложение о криминализации приобретения и хранения вредоносных программ в целях совершения иного преступления?	
a) Полностью поддерживаю, это позволит пресекать преступную деятельность на ранних стадиях (приготовление)	58%
b) Поддерживаю частично, но боюсь, что на практике будет сложно доказать цель совершения иного преступления	29%
c) Не поддерживаю, так как это может привести к необоснованному привлечению к ответственности за «пустое» хранение (коллекционирование, изучение)	12,9%

Считаете ли Вы существующим пробел в уголовном законодательстве РФ и КР в части ответственности за создание сайтов, предназначенных для хранения и распространения вредоносных программ?	
a) Да, пробел существует, действующие статьи не охватывают полностью создание таких ресурсов	54,1%
b) Скорее да, правоприменителям приходится использовать смежные составы или расширительное толкование	34,4%
c) Скорее нет, существующих норм (пособничество, подстрекательство) достаточно	8,2%
d) Нет, пробел отсутствует, такие действия полностью охватываются действующими статьями	3,3%
Согласны ли Вы с необходимостью законодательного закрепления в УК РФ и УК КР положения, исключающего ответственность специалистов по информационной безопасности (white хакеров, тестировщиков) за создание и использование вредоносных программ в рамках их профессиональной деятельности?	
a) Да, это необходимо для исключения рисков необоснованного уголовного преследования	49,2%
b) Скорее да, но с оговоркой, что такие действия не должны нарушать права третьих лиц	37,7%
c) Скорее нет, это создаст лазейки для злоупотреблений	11,5%
d) Нет, все должны нести ответственность по закону независимо от профессии	1,6%
Считаете ли Вы необходимым дополнить диспозиции ст. 273 УК РФ и ст. 320 УК КР указанием на незаконный характер деяний (изложив начало со слова «Незаконные...»), чтобы избежать риска привлечения к ответственности специалистов по информационной безопасности?	
a) Да, это необходимо для разграничения преступных действий и профессиональной деятельности (например, тестирование на проникновение)	68,9%
b) Нет, это избыточно, так как признак незаконности (отсутствия разрешения) подразумевается в самих составах преступлений	18%

c) Да, это важно, но одновременно нужно законодательно закрепить случаи «правомерного использования» вредоносных программ (например, в рамках киберучений)	13,1%
d) Нет, это может создать новые сложности в доказывании умысла	0%
Считаете ли Вы необходимым дополнить ст. 320 УК КР об ответственности за создание, использование и распространение вредоносных программ квалифицирующим признаком «совершение деяния лицом с использованием своего служебного положения»?	
a) Да, это необходимо, так как действия инсайдеров представляют повышенную опасность	59,7%
b) Скорее да, но это может создать сложности в разграничении полномочий сотрудника и его преступных действий	22,6%
c) Скорее нет, действующих норм о должностных преступлениях достаточно для квалификации	6,5%
d) Нет, это избыточно, вредоносная программа опасна сама по себе, независимо от статуса распространителя	6,5%
e) Затрудняюсь ответить	4,8%

ПРИЛОЖЕНИЕ № 2

1166273

КЫРГЫЗ РЕСПУБЛИКАСЫНЫН
БАШКЫ ПРОКУРАТУРАСЫ

ГЕНЕРАЛЬНАЯ ПРОКУРАТУРА
КЫРГЫЗСКОЙ РЕСПУБЛИКИ

720044, Бишкек ш., Токтоналиев көч., 139
тел.: +996 312 542463, факс: 542466
press@prokuror.kg, э/э №12905341131810068
ОКПО 04728939 ИНН 02802199610185

720044, г. Бишкек, ул. Токтоналиева, 139
тел.: +996 312 542463, факс: 542466
press@prokuror.kg, р/с №12905341131810068
ОКПО 04728939 ИНН 02802199610185

06.02.03.10161 № 26/150-9-3-09-680-10108

Российская Федерация,
г.Москва,
ул.Красовского, №2
Вострової А.Н.
vostrovaalesya@yandex.ru

Главное управление информационных технологий и по надзору за исполнением законов в сфере правовой статистики Генеральной прокуратуры Кыргызской Республики, рассмотрев Ваше электронное обращение о предоставлении сведений о статистических данных по количеству совершаемых преступлений с использованием ИКТ и в сфере компьютерных преступлений за 2020-2025 годы для последующего использования в проведении научного исследования – диссертация на соискание ученой степени, сообщает следующее.

За указанный период направляются сведения согласно приложенной таблице:

Период	Ст.319	Ст.320	Ст.321	Ст.322
2021	3	1	2	0
2022	0	0	0	0
2023	0	0	0	0
2024	2	0	0	0
2025	1	7	0	0

Вместе с тем разъясняем, что сведения за 2020 год не представляется возможным предоставить в связи с тем, что в указанный период действовал Уголовный кодекс Кыргызской Республики в редакции от 02.02.2017 года.

Начальник управления **А.Р. Усупбеков**

А.Абдазов
56-70-16 (2006)

ПРИЛОЖЕНИЕ № 3

«Терминологическая модель исследования»

I. ДЕЙСТВУЮЩИЕ ТЕРМИНЫ (de lege lata)
(то, что уже закреплено в законе)

Родовое понятие (РФ) «Компьютерная информация» (ст. 272 УК РФ, прим. 1)	Родовое понятие (КР, перспектива) «Цифровые данные» (п. 98 ст. 1 Цифрового кодекса КР)

ПРЕДМЕТ ПРЕСТУПЛЕНИЯ (de lege lata)

▼ ▼ ▼

Вредоносная компьютерная программа (ст. 273 УК РФ)	Иная вредоносная компьютерная информация (ст. 273 УК РФ + п. 8 ППВС № 37)	вредоносный программный продукт (ст. 320 УК КР) (только программа, без «иной информации»)

II. ПРЕДЛАГАЕМЫЕ ТЕРМИНЫ (de lege ferenda)
(то, что автор предлагает ввести в закон)

▼

ЦИФРОВАЯ ВРЕДОНОСНАЯ ПРОГРАММА
(авторское определение)

• охватывает программы для ЛЮБЫХ цифровых устройств:
- компьютеры, смартфоны, планшеты, IoT, промышленные
- контроллеры, банкоматы, автомобили с цифровым управлением
• заменяет / унифицирует:
- «вредоносная компьютерная программа» (ст. 273 УК РФ)
- «вредоносный программный продукт» (ст. 320 УК КР)

Вводится для решения проблемы: «компьютер» ≠ все цифровые устройства

III. СООТНОШЕНИЕ ТЕРМИНОВ (как это работает)

«Компьютерная информация» (УК РФ)
└── является РОДОВЫМ понятием
├── «Вредоносная компьютерная программа» (вид)
└── «Иная вредоносная компьютерная информация» (вид)

«Цифровые данные» (Цифровой кодекс КР)
└── является РОДОВЫМ аналогом «компьютерной информации»
└──УК КР использует только «программный продукт» (вид)

ПРЕДЛАГАЕТСЯ:
«Цифровая вредоносная программа»
└── универсальный термин de lege ferenda для УК РФ и УК КР
└── замещает устаревшую привязку к «ЭВМ» / «компьютеру»