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

Автореферат

диссертации на соискание ученой степени

кандидата юридических наук

Москва - 2026

Работа выполнена на кафедре уголовного права федерального государственного автономного образовательного учреждения высшего образования «Московский государственный юридический университет имени О.Е. Кутафина (МГЮА)».

Научный руководитель **Русскевич Евгений Александрович**
доктор юридических наук, доцент

Официальные оппоненты: **Бегишев Ильдар Рустамович**
доктор юридических наук, доцент
ЧОУ ВО «Казанский инновационный университет имени В.Г. Тимирясова (ИЭУП)», главный научный сотрудник НИИ цифровых технологий и права, профессор кафедры уголовного права и процесса

Мосечкин Илья Николаевич,
кандидат юридических наук, доцент
ФГБОУ ВО «Вятский государственный университет (ВятГУ)», кафедра уголовного права, процесса и национальной безопасности, доцент кафедры уголовного права, процесса и национальной безопасности

Ведущая организация **ФГКОУ ВО «Московский ордена Почета университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя»**

Защита состоится «04» февраля 2027 года в 14:00 на заседании диссертационного совета 24.2.336.03, созданного на базе ФГАОУ ВО «Московский государственный юридический университет имени О.Е. Кутафина (МГЮА)», г. Москва, 123242, ул. Садовая-Кудринская, д. 7, стр. 22, зал диссертационного совета.

С диссертацией можно ознакомиться в библиотеке и на официальном сайте ФГАОУ ВО «Московский государственный юридический университет имени О. Е. Кутафина (МГЮА)» http://msal.ru.

Автореферат разослан «_____»_____ 20__ г.

Ученый секретарь
диссертационного совета,
доктор юридических наук, профессор А.Н. Першин

ОБЩАЯ ХАРАКТЕРИСТИКА ИССЛЕДОВАНИЯ

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. 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 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. 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.

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 критическую инфраструктуру. 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[1].

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[2]. 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[3]. 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 37 101[4]. 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

---

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

[2] 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).

[3] 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)

[4] 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).

информации зарегистрировано 105 773[5]. 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[6].

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[7]. 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 с вынесением приговора[8]. 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,

---

[5] 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).

[6] 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).

[7] 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).

[8] 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).

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. 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.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обосновывается актуальность темы исследования, раскрывается степень ее научной разработанности, определяются цель и задачи, указываются научная новизна, методология, теоретическая, нормативная и эмпирическая основы работы, формулируются научные положения, выносимые на защиту, раскрывается теоретическая и практическая значимость диссертации, приводятся данные об апробации результатов диссертационного исследования и о его структуре.

Первая глава «Уголовно-правовое противодействие созданию, использованию и распространению вредоносных компьютерных программ: общетеоретический анализ» состоит из трёх параграфов.

В *первом параграфе «Состояние и основные направления противодействия киберпреступности в Российской Федерации и Кыргызской Республики»* установлено, что цифровая трансформация обоих государств сопровождается ростом киберугроз, что предопределяет необходимость адаптации уголовного законодательства к новым вызовам.

В Российской Федерации уголовная-правовая политика в данной сфере эволюционировала от трех статей главы 28 УК РФ, введенных в 1996 году, к развернутой системе из девяти норм, включая ст. 274^{1} УК РФ (неправомерное воздействие на критическую информационную инфраструктуру), ст. 274^{2} УК РФ (нарушение правил централизованного управления сетью «Интернет»), ст. 272^{1} УК РФ (незаконный оборот персональных данных) и новеллы 2025 года – ст.ст. 274^{3}, 274^{4} и 274^{5} УК РФ, криминализирующие незаконное использование абонентских терминалов, организацию деятельности по передаче абонентских номеров и оборот средств доступа к компьютерной информации. Проанализированы позитивные аспекты указанных нововведений, а также выявлены их недостатки, в частности, бланкетный характер ряда норм и риски произвольного толкования.

В Кыргызской Республике уголовная ответственность за компьютерные преступления прошла три этапа: от УК КР 1997 года (ст. 290) через УК КР 2017 года к действующему УК КР 2021 года, в котором ответственность за создание вредоносных программных продуктов предусмотрена ст. 320 УК КР, а глава 28 переименована в главу 40 «Преступления против кибербезопасности», включившую также составы киберсаботажа (ст. 321 УК КР) и массового распространения электронных сообщений (ст. 322 УК КР).

Автором проведен анализ эволюции термина «вредоносная программа» в законодательстве обеих стран, выявлены различия в терминологических подходах, а также отмечено отсутствие в Кыргызской Республике официальных разъяснений высшей судебной инстанции по применению ст. 320 УК КР, в отличие от постановления Пленума Верховного Суда РФ от 15.12.2022 № 37, конкретизирующего положения главы 28 УК РФ.

Во *втором параграфе «Международные стандарты противодействия киберпреступности»* исследованы ключевые международно-правовые акты, формирующие глобальную и региональную архитектуру борьбы с киберпреступностью.

Особое внимание уделено Будапештской конвенции 2001 года, которая закрепила четыре группы преступлений (против конфиденциальности, целостности и доступности данных; с использованием компьютерных систем как орудия; связанные с содержанием данных; нарушающие авторские права) и процессуальные механизмы сотрудничества. Отмечено, что Российская Федерация, подписав, но не ратифицировав указанную Конвенцию, критикует ее за недостаточный учет принципа государственного суверенитета. В этой связи проанализирована российская инициатива по разработке универсальной Конвенции ООН против киберпреступности, утвержденной Генеральной Ассамблеей ООН 24 декабря 2024 года и открытой для подписания 25 октября 2025 года, в которой, в отличие от Будапештской конвенции 2001 года, акцент сделан на невмешательство во внутренние дела и исключение прямого трансграничного доступа к данным без согласия государства.

Проведен сравнительный анализ соответствия ст. 273 УК РФ и ст. 320 УК КР положениям ст. 7-11 Конвенции ООН против киберпреступности (далее – Конвенция), в результате которого выявлено, что: а) ст. 273 УК РФ и ст. 320 УК КР в целом коррелируют с нормой пп. «а» п. 1 ст. 11 и, однако объективная сторона ограничена созданием, использованием и распространением, тогда как Конвенция требует криминализации также получения, производства, продажи, приобретения, ввоза и предоставления иным способом; б) в законодательстве обеих стран отсутствует прямое указание на уголовную ответственность за владение (хранение) вредоносными программами, что требуется пп. «в» п. 1 ст. 11 Конвенции; в) российский законодатель в 2025 году ввел ст. 274^5 УК РФ, криминализующую оборот паролей, реквизитов доступа и электронной подписи, что обеспечило имплементацию пп. «а» (ii) п. 1 ст. 11 Конвенции, тогда как в Кыргызской Республике соответствующая норма отсутствует, что создает существенный пробел; г) ст. 321 УК КР о киберсаботаже текстуально соответствует положению ст. 10 Конвенции о серьезном препятствовании функционированию системы, тогда как российское законодательство в этой части является более узким. Кроме того, рассмотрены региональные инструменты: Соглашение ШОС 2009 года, Соглашение СНГ 2001 года и его обновленная версия 2018 года, Конвенция ЛАГ 2010 года и Малабская конвенция Африканского союза 2014 года, а также позиция стран БРИКС.

В третьем параграфе «Ответственность за действия с вредоносными компьютерными программами по законодательству стран Содружества Независимых Государств» проведен сравнительно-правовой анализ уголовных кодексов девяти государств СНГ (России, Кыргызстана, Казахстана, Таджикистана, Беларуси, Узбекистана, Азербайджана, Армении, Туркменистана и Молдовы). Установлено, что при общем сходстве подходов, обусловленном общим советским правовым наследием, национальные законодательства демонстрируют значительные различия в конструировании объективной стороны, определении круга криминализируемых действий, конструкции состава и системе квалифицирующих признаков.

В части объективной стороны выявлено, что законодатели Кыргызстана, Казахстана, Таджикистана, Туркменистана и Узбекистана включают в диспозицию «внесение изменений в существующие программы» как самостоятельное действие, тогда как в ст. 273 УК РФ такие изменения не упоминаются, что, по мнению автора, создает сложности при квалификации модификации легального программного обеспечения. Белорусский законодатель дополнительно криминализирует «сбыт» вредоносных программ, а азербайджанский – ввоз, приобретение, продажу, распространение и создание условий для приобретения. В части конструкции составов выявлено, что в большинстве стран (Россия, Казахстан, Таджикистан, Армения, Узбекистан, Беларусь, Туркменистан) основной состав является формальным, тогда как в Кыргызстане (ст. 320 УК КР) и Азербайджане (ст. 273-1 УК) – материальным, требующим наступления значительного ущерба или иного значительного вреда.

Автором обоснована позиция, согласно которой формальная конструкция более эффективна для противодействия обороту вредоносного инструментария, тогда как материальный состав оставляет безнаказанными действия по созданию и распространению вредоносных программ, не повлекших последствий. В части квалифицирующих признаков отмечено, что ряд государств (Казахстан, Кыргызстан, Туркменистан) выделяют в качестве особо квалифицирующего признака совершение деяния в отношении критической информационной инфраструктуры.

В части предмета преступления выявлено, что Азербайджан и Молдова криминализируют оборот паролей и кодов доступа, Россия ввела такую ответственность ст. 274^5 УК РФ, тогда как в Кыргызстане соответствующий пробел сохраняется.

В отношении субъективной стороны установлено, что во всех анализируемых государствах преступление совершается с прямым умыслом, при этом в квалифицированных составах ряда стран (Россия, Армения) предусмотрена корыстная заинтересованность как отягчающий признак. Субъект преступления – физическое вменяемое лицо с 16 лет, за исключением Молдовы, где

ответственность по ст. 260 УК наступает с 14 лет и предусмотрена ответственность юридических лиц.

Вторая глава «Уголовно-правовая характеристика создания, использования и распространения вредоносных компьютерных программ по законодательству Российской Федерации и Кыргызской Республики» состоит из трёх параграфов.

В *первом параграфе «Объект создания, использования и распространения вредоносных компьютерных программ (ст. 273 УК РФ, ст. 320 УК КР)»* установлено, что родовым объектом как для российской, так и для кыргызской нормы являются общественные отношения в сфере обеспечения общественной безопасности и общественного порядка, что обусловлено расположением соответствующих статей в главах 28 и 40 УК соответственно.

В отношении видового объекта в российской доктрине наблюдается дискуссия: от узкого понимания как безопасности информации и нормального порядка функционирования компьютерных систем до широких трактовок, включающих всю совокупность общественных отношений в информационной сфере, или состояние защищенности личности, общества и государства от информационных угроз. В кыргызской доктрине видовой объект определяется как информационная безопасность как вид общественной безопасности.

На основе анализа Доктрины информационной безопасности Российской Федерации и Концепции национальной безопасности Кыргызской Республики автором предложено авторское определение видового объекта как общественных отношений, обеспечивающих цифровую безопасность как неотъемлемый элемент общественной безопасности, гарантирующих 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.

Особое внимание уделено предмету преступления. В российской доктрине предмет ст. 273 УК РФ трактуется по-разному: от узкого понимания как

вредоносной программы для ЭВМ до широкого, включающего компьютерную информацию, вредоносную компьютерную программу или иную компьютерную информацию, а также средства защиты компьютерной информации. Автором обоснована позиция, что предмет преступления по ст. 273 УК РФ является альтернативным: либо вредоносная компьютерная программа, либо иная вредоносная компьютерная информация, при этом «вредоносность» является обязательным юридическим свойством, определяемым не техническими характеристиками кода, а заведомой предназначенностью программы для совершения указанных в диспозиции действий.

В отношении ст. 320 УК КР установлено, что законодатель использует термин «программный продукт», который, по мнению автора, не расширяет предмет на любую компьютерную информацию, а подчеркивает завершенность объекта как готового к использованию инструмента, что подтверждается системным соотношением со ст. 319 УК КР, где законодатель отдельно оперирует понятием «компьютерная информация». При этом выявлено существенное отличие в описании вредоносного потенциала: в ст. 320 УК КР перечень вредоносных действий расширен за счет указания на «несанкционированный доступ и копирование» и «нарушение работы информационных систем или сети электросвязи», что делает диспозицию более широкой по сравнению со ст. 273 УК РФ.

На основе анализа современной цифровой среды, включая IoT-устройства, киберфизические системы и облачные платформы, автором предложено ввести в научный и практический оборот универсальное понятие **«цифровая вредоносная программа»** – *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 устройства или сети.* Данное определение, по мнению автора, позволит преодолеть узость традиционного подхода, привязанного к «программам для ЭВМ», и обеспечить адекватную правовую

защиту всей цифровой экосистемы. Проанализирована категория «иная вредоносная компьютерная информация» в контексте ст. 273 УК РФ, включая разъяснения Пленума Верховного Суда РФ от 15.12.2022 № 37 (ключи доступа, элементы кодов), доктринальные подходы и судебную практику. В отношении Кыргызской Республики сделан вывод, что Цифровой кодекс КР создает предпосылки для расширительного толкования предмета ст. 320 УК КР, включая ключи, метаданные и иные цифровые записи, однако требуется законодательная конкретизация.

Во *втором параграфе «Объективная сторона создания, использования и распространения вредоносных компьютерных программ (ст. 273 УК РФ, ст. 320 УК КР)»* проведен детальный анализ альтернативных действий, образующих объективную сторону. В части создания установлено, что российская доктрина и судебная практика (п. 9 постановления Пленума ВС РФ № 37, Методические рекомендации Генпрокуратуры) трактуют создание максимально широко: как деятельность по разработке или подготовке вредоносных программ, включая модификацию существующих, при этом преступление считается оконченным с момента начала осуществления любого из этапов разработки (постановка задачи, написание кода, отладка, тестирование). Ключевым критерием является изначальная предназначенность программы для деструктивных действий. В ст. 320 УК КР создание не имеет законодательного определения, однако на основе системного анализа автором предложено понимать его как целенаправленную деятельность по разработке программного продукта, результатом которой является появление объекта, пригодного для вредоносного воздействия, при этом создание не требует доведения программы до полной готовности.

Ключевым отличием объективной стороны по ст. 320 УК КР является включение в диспозицию четвертого альтернативного действия – «внесение изменений в существующие программные продукты», которое было исключено из ст. 273 УК РФ в 2011 году. Автором обоснована позиция, что кыргызский подход является более широким и прогрессивным, поскольку криминализирует модификацию существующего программного обеспечения как самостоятельный

способ совершения преступления, что позволяет более гибко квалифицировать действия злоумышленников, активно использующих методы доработки и адаптации уже существующих кодов.

В части конструкции состава выявлено принципиальное различие: ст. 273 УК РФ в основном составе сконструирована как формальная, преступление считается оконченным с момента совершения любого из указанных действий, независимо от наступления последствий; квалифицированные составы (ч. 2, 3) являются формально-материальными, требующими либо крупного ущерба (ч. 2), либо тяжких последствий или угрозы их наступления (ч. 3). В отличие от этого, ст. 320 УК КР демонстрирует эволюцию от формального состава (УК 1997 г. и 2017 г.) к формально-материальному в действующей редакции 2021 г.: создание и внесение изменений наказуемы независимо от последствий (формальный состав), тогда как использование и распространение требуют наступления значительного ущерба (материальный признак).

В *третьем параграфе «Субъективные признаки создания, использования и распространения вредоносных компьютерных программ (ст. 273 УК РФ, ст. 320 УК КР)»* проведен анализ субъективной стороны и субъекта преступления. В части субъективной стороны установлено, что в российской доктрине субъективная сторона ст. 273 УК РФ характеризуется прямым умыслом: виновный осознает общественную опасность своих действий, понимает заведомую вредоносность программы и желает совершить деяние. Квалифицированный состав ч. 3 ст. 273 УК РФ может характеризоваться двумя формами вины, когда к прямому умыслу на совершение деяния добавляется неосторожное отношение к тяжким последствиям. Мотив и цель являются факультативными признаками для основного состава, однако они учитываются при назначении наказания и могут приобрести обязательное значение, если преступление является способом совершения иного, более тяжкого деяния.

В кыргызской доктрине субъективная сторона ст. 320 УК КР также характеризуется прямым умыслом, однако имеется дискуссия о возможности косвенного умысла. Ключевым отличием является наличие в ст. 320 УК КР

специальной цели – «создание с целью использования либо распространения», что делает цель конструктивным, обязательным признаком субъективной стороны для действия «создание», в отличие от российского подхода, где цель является факультативной. Автором обосновано, что указание на специальную цель, с одной стороны, усиливает гарантии для добросовестных исследователей, но с другой – создает дополнительные сложности для обвинения в доказывании субъективной стороны. Автором предлагается практический алгоритм установления субъективной стороны через анализ объективных обстоятельств.

В части субъекта преступления установлено, что как по ст. 273 УК РФ, так и по ст. 320 УК КР субъектом является общий – физическое вменяемое лицо, достигшее 16-летнего возраста. Однако в квалифицированном составе ч. 2 ст. 273 УК РФ содержится признак «совершение деяния лицом с использованием своего служебного положения», что превращает субъекта в специального. В ст. 320 УК КР аналогичный квалифицирующий признак отсутствует. Автор обосновывает необходимость дополнения ст. 320 УК КР квалифицирующим признаком «совершение деяния лицом с использованием своего служебного положения», что позволит адекватно оценивать повышенную общественную опасность деяний, совершаемых инсайдерами, обладающими особым доступом к информационным системам в силу должностных обязанностей.

Третья глава «Перспективные направления совершенствования законодательства и проблемы квалификации создания, использования и распространения вредоносных компьютерных программ» состоит из двух параграфов.

В *первом параграфе «Особенности и проблемы квалификации создания, использования и распространения вредоносных компьютерных программ»* исследованы наиболее дискуссионные и практически значимые вопросы правоприменения. Установлено, что ключевой проблемой квалификации является отсутствие легальных дефиниций понятий «вредоносная компьютерная программа» и «вредоносный программный продукт», что порождает зависимость судебных решений от результатов компьютерно-технических экспертиз,

методологии которых могут существенно различаться. В результате один и тот же программный код может получать различную правовую оценку, что создает риски как необоснованного привлечения к ответственности, так и ухода от нее реальных преступников. Применительно к Кыргызской Республике выявлена проблема отсутствия систематизированной открытой судебной практики по ст. 320 УК КР. В качестве эмпирического замещения проанализированы инциденты из открытых источников: хакерская атака на сайт Государственной налоговой службы КР в 2023 г., трояны XPath и Mirage, выявленные в сетях госучреждений, утечка персональных данных 600 тыс. граждан через SQL-инъекцию, а также статистика «Лаборатории Касперского» о том, что каждый 30-й компьютер в Кыргызстане атакован вредоносным программным обеспечением. Сделан вывод, что фактическая распространенность вредоносных программ в Кыргызстане высока, однако отсутствие правоприменительной практики создает серьезные препятствия для единообразного применения закона и международного сотрудничества.

На основе анализа судебной практики Российской Федерации выявлены следующие проблемные аспекты. Во-первых, в отсутствие четких законодательных дефиниций суды вынуждены определять «вредоносность» программы ситуативно, через совокупность объективных обстоятельств. Во-вторых, острой дискуссионной проблемой является квалификация VPN-сервисов: анализ практики показывает наличие расширительного толкования, однако большинство судебных решений последовательно исходят из того, что легитимный VPN-сервис, обеспечивающий шифрование трафика и смену IP-адреса, не является вредоносной программой по смыслу ст. 273 УК РФ; для признания программы вредоносной требуется установление деструктивного функционала, подтвержденного экспертизой. В-третьих, проанализирована практика привлечения к ответственности за создание и распространение читов и ботов для многопользовательских онлайн-игр, где вредоносность выражается в несанкционированной модификации защищенного кода нейтрализации средств «античита», что подтверждает возможность квалификации таких деяний по ст. 273 УК РФ. Отмечена эволюция угроз в сфере гейминга.

Особое внимание уделено проблеме разграничения ст. 272 УК РФ и ст. 273 УК РФ, а также вопросы разграничения ст. 273 УК РФ и ст. 138^1 УК РФ (незаконный оборот специальных технических средств), где ключевым критерием признается наличие деструктивного функционала: программное обеспечение, предназначенное исключительно для скрытого получения информации, но не содержащее средств нейтрализации защиты и не направленное на уничтожение, блокирование или модификацию данных, не отвечает признакам вредоносной программы по ст. 273 УК РФ. Сделан вывод о необходимости более четких разъяснений со стороны высших судебных инстанций.

Во *втором параграфе «Основные направления совершенствования уголовного законодательства Российской Федерации и Кыргызской Республики об ответственности за создание, использование и распространение вредоносных компьютерных программ»* сформулированы научно обоснованные предложения по развитию уголовно-правовых норм. Обоснована необходимость расширения предмета ст. 320 УК КР по модели ст. 273 УК РФ путем включения наряду с вредоносным программным продуктом также иной вредоносной компьютерной информации, что позволит охватить такие современные угрозы, как скрипты, макросы, измененные данные управления, не образующие самостоятельной программы, но обладающие деструктивным потенциалом.

Аргументирована необходимость криминализации приобретения и (или) хранения вредоносных программ в целях совершения иного преступления, которые в настоящее время остаются вне сферы действия уголовного закона, что создает ситуацию, когда лицо, целенаправленно покупающее вирус для последующего применения, формально не подпадает под действие уголовного закона до момента начала активных действий.

Предложено криминализировать создание и обеспечение функционирования информационных ресурсов (сайтов, страниц, каналов), заведомо предназначенных для незаконного хранения, передачи или распространения вредоносных программ, что позволит привлекать к ответственности организаторов криминальных онлайн-платформ, которые в

настоящее время остаются вне поля действия уголовного закона, несмотря на их ключевую роль в современных киберпреступных экосистемах.

Обозначена перспективная проблема противодействия вредоносным программам на основе технологий искусственного интеллекта, которые обладают принципиально новыми свойствами – адаптивностью, способностью к самообучению, автономностью, вариативностью действий и способностью заменять сложное соучастие в совершении преступления. Отмечено, что Кыргызская Республика уже сделала важный шаг в признании новых технологических угроз на уровне цифрового законодательства, закрепив легальное определение *дипфейка* в Цифровом кодексе КР, однако уголовное законодательство обеих стран в этой части остается неразработанным, что требует дальнейших научных исследований и законодательных решений.

В **заключении** диссертации подводятся итоги проведенного исследования, формулируются его основные положения и выводы.

В **приложениях** приведены результаты социологического опроса, а также представлена схема «Терминологическая модель исследования» предмета преступления, предусмотренного ст. 273 УК РФ и ст. 320 УК КР.

Основные положения диссертации отражены в следующих работах автора (общим объемом 3,94 п. л.):

Публикации в рецензируемых научных изданиях, включенных Высшей аттестационной комиссией при Министерстве науки и высшего образования Российской Федерации в перечень рецензируемых научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук:

1. Вострова, А.Н. Сравнительно-правовой анализ объективной стороны преступлений, связанных с оборотом вредоносных программ, по уголовному законодательству Российской Федерации и Кыргызской Республики / А.Н. Вострова // Полицейская и следственная деятельность. – 2026. – № 1. – С. 250-262. (0,97 п.л.).

2. Вострова, А.Н. Уголовно-правовая политика Киргизской Республики в сфере противодействия киберпреступности: анализ эволюции законодательства / А.Н. Вострова // Искусство правоведения. The art of law. – 2026. – № 1. – С. 89-94. (0,43 п.л.).

3. Вострова, А.Н. Объект и предмет преступлений, связанных с созданием, использованием и распространением вредоносных компьютерных программ: сравнительно-правовой анализ по законодательству Российской Федерации и Киргизской Республики / А.Н. Вострова // Вестник Московской академии Следственного комитета Российской Федерации. – 2025. – № 4. С. 127-134. (0,85 п.л.).

4. 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. (0,51 п.л.).

Публикации в иных изданиях:

5. Вострова, А.Н. К вопросу о разграничении составов преступлений, предусмотренных статьями 138^1 и 273 Уголовного кодекса Российской Федерации / А.Н. Вострова // Стратегия противодействия преступности в изменяющемся мире: к 95-летию со дня рождения профессора Г.И. Чечеля: Сборник материалов Всероссийской (национальной) научно-практической конференции. – Ставрополь: Изд-во СКФУ. – 2026. – С. 54-59. (0,34 п.л.).

6. Вострова, А.Н. Уголовная ответственность за действия с вредоносными программами в странах БРИКС / А.Н. Вострова // Цифровые технологии и право: Сборник научных трудов IV Международной научно-практической конференции, Казань, 19 сентября 2025 года. – Казань: Познание. – 2026. – Т. 9. – С. 71-80. (0,6 п.л.).

7. Вострова, А.Н. Уголовная ответственность за действия с вредоносными компьютерными программами по законодательству Российской Федерации и Кыргызской Республики / А.Н. Вострова // Уголовная политика в условиях цифровой трансформации: Сборник статей материалов III Всероссийской научно-практической конференции, Казань, 18–19 апреля 2024 года. – Казань: Отечество. – 2024. – С. 23-27. (0,24 п.л.).