



Министерство внутренних дел Российской Федерации
Омская академия

На правах рукописи

Карабеков Канатбек Омирзакович

**Киберпреступность
в Российской Федерации
и Республике Казахстан:
состояние и меры предупреждения**

Специальность 5.1.4. Уголовно-правовые науки

*Автореферат
диссертации на соискание ученой степени
кандидата юридических наук*

Омск 2025

Работа выполнена в федеральном государственном казенном образовательном учреждении высшего образования «Омская ордена Почета академия Министерства внутренних дел Российской Федерации».

Научный руководитель:

Бабурин Василий Васильевич, Заслуженный работник высшей школы Российской Федерации, доктор юридических наук, профессор, профессор кафедры криминологии и профилактики преступлений федерального государственного казенного образовательного учреждения высшего образования «Омская ордена Почета академия Министерства внутренних дел Российской Федерации»

Официальные оппоненты:

Бегишев Ильдар Рустамович, доктор юридических наук, доцент, профессор кафедры уголовного права и процесса частного образовательного учреждения высшего образования «Казанский инновационный университет имени В. Г. Тимирязова (ИЭУП)»;

Сидорова Екатерина Закариевна, кандидат юридических наук, доцент, заместитель начальника кафедры уголовного права и криминологии федерального государственного казенного образовательного учреждения высшего образования «Восточно-Сибирский институт Министерства внутренних дел Российской Федерации» (г. Иркутск)

Ведущая организация:

федеральное государственное бюджетное образовательное учреждение высшего образования «Кубанский государственный университет» (г. Краснодар)

Защита состоится 12 декабря 2025 г. в 13:00 часов на заседании диссертационного совета 03.2.010.01, созданного на базе федерального государственного казенного образовательного учреждения высшего образования «Омская ордена Почета академия Министерства внутренних дел Российской Федерации» по адресу: 644092, г. Омск, пр-т Комарова, д. 7, зал заседаний ученого совета.

С диссертацией можно ознакомиться в библиотеке и на сайте федерального государственного казенного образовательного учреждения высшего образования «Омская ордена Почета академия Министерства внутренних дел Российской Федерации» (<http://www.omamvd.ru/diss/>).

Автореферат разослан «___» октября 2025 г.

Ученый секретарь
диссертационного совета
кандидат юридических наук,
доцент



Ларин Евгений Геннадьевич

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. Киберпреступность представляет собой крайне опасное явление современности, свойственное многим развитым в информационном отношении государствам, в том числе Российской Федерации и Республике Казахстан. На сегодняшний день в Российской Федерации 88,0% населения пользуется интернетом, в Республике Казахстан этот показатель достигает 89,2%. Статистика демонстрирует, что с увеличением количества интернет-пользователей в наших странах растет и число киберпреступлений, причиняющих значительный ущерб как гражданам, так и государству.

Результаты исследования свидетельствуют, что к настоящему моменту правоохранные органы России и Казахстана в целом оказались не готовы к предупреждению такого общественно опасного явления, как киберпреступность, своевременно не осознав реальные угрозы, исходящие от действий киберпреступников, не определив основные тенденции развития киберпреступности. Способы совершения киберпреступлений настолько быстро меняются, приобретают более новые формы и проявляются во многих сферах жизнедеятельности общества и государства (кибершпионаж, интернет-мошенничество и пр.), что уголовно-правовое регулирование не всегда успевает за скоростью преобразования указанных преступлений, а дополнения в уголовное законодательство в части борьбы с новыми видами киберпреступлений вносятся с запозданием. Соответственно, правоприменительные органы не располагают актуальными уголовно-правовыми средствами борьбы с киберпреступлениями.

Сложная ситуация складывается и с вопросами организации предупреждения данных видов преступлений. Пока киберпреступность становится все более актуальной и серьезной социальной угрозой, правоприменительная и предупредительная деятельность правоохранительных органов во многом не соответствуют темпам роста преступной активности в киберпространстве.

О том, что современная киберпреступность — значительная проблема, угрожающая имущественным и иным интересам физических и юридических лиц, безопасности общества и государства, отмечается в наших странах на самом высоком государственном уровне.

Так, Президент Российской Федерации Владимир Путин 2 апреля 2024 г. в ходе выступления на ежегодном расширенном заседании коллегии Министерства внутренних дел назвал показатели преступлений в кибер-

пространстве впечатляющими: «Почти на 30% выросло число преступлений с использованием информационных технологий. Их совершено порядка 680 тысяч, а ущерб превысил 156 миллиардов рублей». По его словам, борьба с киберпреступностью в стране — один из безусловных приоритетов работы российских правоохранительных органов. Среди мер борьбы с данным видом преступлений глава Российского государства назвал профилактику: «Нужно серьезно совершенствовать механизмы борьбы с правонарушениями в этой сфере, работать на опережение».

22 января 2024 г. под председательством Президента Республики Казахстан Касым-Жомарта Токаева состоялось расширенное заседание коллегии МВД, где глава государства отметил, что правоохранительные органы должны вести решительную борьбу с интернет-мошенниками, жертвами которых становятся многие граждане, и поручил МВД РК поставить заслон киберпреступности и интернет-мошенничеству.

Пристальное внимание глав наших государств к проблеме киберпреступности подчеркивает ее особую актуальность и определяет необходимость системного и всестороннего исследования этого феномена.

Актуальность сравнительного анализа состояния и мер предупреждения киберпреступности в России и Казахстане также обусловливается рядом других факторов.

Во-первых, это рост уровня киберугроз для деятельности соседних государств, связанных совместными обязательствами по оказанию помощи в борьбе с преступностью. Российская Федерация и Республика Казахстан являются странами Содружества Независимых Государств, непосредственно сталкивающимися с ростом уровня киберпреступности. В обеих странах увеличивается число случаев кибершпионажа, кибератак на государственные и коммерческие объекты, кибермошенничества и распространения вредоносного программного обеспечения. Сравнительный анализ роста уровня киберугроз двух стран позволит выявить особенности киберпреступности в наших странах и ее общие тенденции, а также выработать единые подходы в ее предупреждении.

Во-вторых, ближайшее соседство Российской Федерации и Республики Казахстан определяет, что киберпреступность для наших стран является трансграничной, в связи с чем обусловливается необходимость постоянного взаимодействия соседних правоохранительных органов в борьбе с ней, обмена информацией о киберпреступности и опытом борьбы с указанной преступностью. Проведение сравнительного анализа позволит выявить передовой положительный опыт наших стран по предупреждению киберпреступности, раскрыть содержание мер повышения эффективности работы правоохранительных органов в этом направлении. Так, в Казахстане такие

меры включают в себя цифровизацию всей правоохранительной системы и переход на электронный формат ведения уголовных дел.

В-третьих, с учетом близости и сходства исторических, культурных и экономических связей между Россией и Казахстаном высока потребность в укреплении совместной безопасности государств, и прежде всего в сфере кибербезопасности. Россия и Казахстан активно работают над укреплением собственной кибербезопасности и предотвращением кибератак, но остаются нерешенными вопросы взаимодействия в борьбе с данным видом преступности. Здесь имеются большие резервы в организации правового обеспечения совместной деятельности государств по предупреждению киберпреступлений. Сравнительный анализ позволит выявить основные проблемы взаимодействия в противодействии киберпреступности, разработать совместные стратегии борьбы с киберугрозами.

В-четвертых, Россия и Казахстан продолжают опережающее развитие своих киберинфраструктур, что в современных условиях требует совместных усилий, направленных на анализ реальной опасности возрастающих киберугроз, что является необходимым условием предупреждения рассматриваемых видов преступлений. Сравнительный анализ поможет оценить уровень кибербезопасности в обеих странах, выявить потенциальные проблемы, связанные с киберпреступлениями, предложить пути их решения.

С учетом изложенного налицо острая необходимость в криминологической оценке современного состояния и тенденций киберпреступности в Российской Федерации и Республике Казахстан и разработке на этой основе согласованных мер ее предупреждения, что подтверждает актуальность темы диссертационного исследования.

Степень разработанности темы исследования. Изучением вопросов криминологической характеристики преступлений и предупреждения преступности занимались многие российские и казахстанские ученые. Так, вопросам анализа состояния и мер предупреждения преступности посвящены научные труды Г. А. Аванесова, Е. О. Алауханова, Ю. М. Антоняна, В. В. Бабурина, С. Е. Вицина, У. С. Джекебаева, А. И. Долговой, С. М. Иншакова, Е. И. Каиржанова, М. П. Клейменова, Н. Ф. Кузнецовой, С. Я. Лебедева, В. В. Лунеева, И. М. Мацкевича, В. Д. Малкова, В. И. Омигова, А. В. Петровского, Л. М. Прокументова, А. Л. Репецкой, Н. А. Стручкова, А. В. Шеслера, Д. А. Шестакова и др.

Исследованием проблем предупреждения киберпреступлений занимались такие российские и казахстанские ученые, как И. Р. Бегишев, Р. Е. Джансараева, В. Ф. Джафарли, А. Т. Исмагулова, И. М. Глотина, П. Н. Кобец, А. Д. Мухамеджанова, В. А. Номоконов, А. Л. Осипенко, Т. В. Пинкевич, Д. В. Пучков, Г. Р. Рустимова, Е. З. Сидорова и др.

Среди исследований российских и казахстанских ученых, посвященных разработке транснациональных аспектов киберпреступности, можно отметить диссертации: Б. Х. Толеубековой «Проблемы совершенствования борьбы с преступлениями, совершаемыми с использованием компьютерной техники» (Алматы, 1998); Т. Б. Сеитова «Международно-правовое сотрудничество государств в борьбе с компьютерной преступностью» (Алматы, 2002); А. А. Жмыхова «Компьютерная преступность за рубежом и ее предупреждение» (Москва, 2003), Т. Л. Тропиной «Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы» (Владивосток, 2005); Т. М. Лопатиной «Криминологические и уголовно-правовые основы противодействия компьютерной преступности» (Москва, 2006); А. К. Нурпеи-совой «Уголовно-правовые и криминалистические аспекты компьютерной преступности» (Караганда, 2010); К. Аратулы «Уголовная политика в борьбе с компьютерной преступностью в условиях глобализации» (Алматы, 2013); И. Г. Чекунова «Криминологическое и уголовно-правовое обеспечение предупреждения киберпреступности» (Москва, 2013); М. А. Простосердова «Экономические преступления, совершаемые в киберпространстве, и меры противодействия им» (Москва, 2016), К. Н. Евдокимова «Противодействие компьютерной преступности: теория, законодательство, практика» (Москва, 2022), Е. А. Родиной «Противодействие криминальной виктимизации пользователей сети „Интернет“ в киберпространстве» (Саратов, 2022), Д. А. Конева «Криминологическая безопасность и ее обеспечение в сфере цифровых технологий» (Омск, 2022).

Несмотря на наличие ряда работ российских и казахстанских ученых, посвященных совершенствованию уголовной ответственности за совершение компьютерных преступлений, актуальными остаются вопросы исследования нормативно-правового регулирования борьбы с киберпреступностью в странах Содружества Независимых Государств, прежде всего в России и Казахстане. Особого внимания требуют аспекты изучения состояния киберпреступности в указанных странах, опыта ее предупреждения.

Объект и предмет исследования. Объектом диссертационного исследования являются общественные отношения, возникающие в связи с совершением киберпреступлений в Российской Федерации и Республике Казахстан, определяющие особенности состояния такой преступности и меры ее предупреждения в данных странах.

Предмет исследования составляют киберпреступность в Российской Федерации и Республике Казахстан, ее состояние и динамика, процессы и явления, детерминирующие киберпреступность, правовое регулирование и практика предупреждения киберпреступлений в Российской Федерации и Республике Казахстан.

Цель и задачи исследования. Цель диссертационного исследования заключается в получении нового научного знания о криминологической характеристике современных киберпреступлений, совершаемых в Российской Федерации и Республике Казахстан, и разработке на этой основе предложений по совершенствованию мер предупреждения преступлений данного вида в указанных странах.

Достижение изложенной цели потребовало постановки и решения следующих задач:

- сформулировать понятие и определить криминологическую природу киберпреступности в Российской Федерации и Республике Казахстан;
- осуществить анализ состояния киберпреступности в Российской Федерации и Республике Казахстан, определить ее основные тенденции;
- выделить особенности лиц, совершивших киберпреступления;
- выявить детерминанты киберпреступности в Российской Федерации и Республике Казахстан;
- разработать меры правового обеспечения предупреждения киберпреступности;
- определить основные направления совершенствования мер предупреждения киберпреступлений в Российской Федерации и Республике Казахстан.

Теоретическую основу исследования составили фундаментальные работы ученых в области криминологии, уголовного права, иных отраслей наук. В диссертации проанализированы научные воззрения ученых, изложенные в монографических и диссертационных исследованиях, научных статьях, посвященных вопросам определения криминологической характеристики и предупреждения киберпреступлений.

Научная новизна исследования заключается в разработке авторского подхода к определению киберпреступности, в обосновании основных признаков, определяющих содержание киберпреступности, раскрытии содержания ее криминологической природы, определении специфики современного состояния киберпреступности в Российской Федерации и Республике Казахстан, в выделении особенностей личности киберпреступника, в формулировании классификации основных видов киберпреступников.

По итогам сравнительного криминологического анализа состояния киберпреступности выявлены ее закономерности и тенденции в России и Казахстане. Определены детерминанты киберпреступности в данных государствах. Проведена оценка практики обеспечения криминологической кибербезопасности в указанных странах, в том числе при реализации программ и планов регионального характера. Разработаны научно обоснованные рекомендации по предупреждению противоправного поведения кибер-

преступников и защите населения от киберугроз. По результатам исследования сформулированы предложения по совершенствованию мер предупреждения киберпреступности.

Теоретическая и практическая значимость исследования состоит в том, что полученные научные результаты дополняют теоретическую базу понятия киберпреступности, и ее признаков. Характеристика современного состояния киберпреступности в России и Казахстане, его тенденций вносит существенный вклад в решение проблемы предупреждения киберпреступлений в данных странах. В работе выделены особенности личности киберпреступников корыстной направленности, раскрыто содержание современных социально-экономических, организационно-технических, правовых, международных детерминант киберпреступности, а также предложены конкретные меры предупреждения киберпреступности в Российской Федерации и Республике Казахстан.

Практическое значение результатов настоящего исследования состоит в научно обоснованных рекомендациях и иных исследовательских материалах, которые могут быть использованы правоохранительными органами России и Казахстана для своевременного прогнозирования состояния киберпреступности в данных странах, выявления и предупреждения киберпреступлений, прежде всего корыстной направленности; в законодательской деятельности, в научно-исследовательской деятельности, в учебном процессе образовательных организаций высшего образования.

Полученные результаты исследования могут быть использованы в образовательном процессе вузов системы МВД России при изучении учебных дисциплин «Криминология», «Предупреждение преступлений и административных правонарушений органов внутренних дел».

Методология и методы исследования. Достоверность и объективность выводов проведенного исследования обеспечены применением диалектического и основанных на нем общенаучных и частнонаучных методов познания.

При определении понятия и признаков киберпреступности, обосновании ее предпосылок, а также мер ее предупреждения применялся формально-юридический метод (в сочетании с синтезом, индукцией и дедукцией).

Сравнительно-правовой метод использовался при анализе особенностей правового обеспечения предупреждения киберпреступности в России и Казахстане, организации деятельности правоохранительных органов по предупреждению корыстных киберпреступлений.

Статистические методы (сводка, группировка, статистический анализ, моделирование), опрос (в виде анкетирования, интервьюирования) позволили проанализировать состояние, структуру и тенденции киберпре-

ступности, определить положительный опыт в предупреждении киберпреступлений корыстной направленности, совершаемых с использованием информационно-телекоммуникационных технологий, а также выделить ключевые проблемы на пути к их эффективному предупреждению.

Системно-структурный метод и метод анализа позволили классифицировать: совокупность киберпреступлений корыстной направленности, совершаемых с использованием информационно-телекоммуникационных технологий; личностные особенности киберпреступников; детерминанты киберпреступлений в России и Казахстане; предпосылки и меры предупреждения киберпреступлений в данных странах.

Положения, выносимые на защиту.

1. Под киберпреступностью в Российской Федерации и Республике Казахстан следует понимать исторически изменчивое, обладающее повышенной латентностью социальное и уголовно-правовое негативное явление, представляющее собой систему преступлений, совершенных дистанционно в информационном пространстве с использованием средств информационно-телекоммуникационных технологий. Современное содержание киберпреступности в России и Казахстане определяется совокупностью разнородных преступлений (уголовных правонарушений в РК), имеющих особую поведенческую природу образования, включающую в себя общественно опасное использование компьютерной информации и информационно-телекоммуникационных технологий в целях удовлетворения потребностей преимущественно корыстной направленности.

2. Основные криминологические показатели киберпреступности указывают на то, что уровень, структура и динамика киберпреступности в Российской Федерации и Республике Казахстан имеют существенные отличия. Прежде всего, отличие проявляется в доле киберпреступлений в общей массе преступности. Так, несмотря на высокий уровень цифровизации в Казахстане, данные свидетельствуют о меньшем уровне киберпреступности там по сравнению с Россией. В расчете на единицу населения в Российской Федерации киберпреступлений совершается в три раза больше, чем соответствующих уголовных правонарушений в Республике Казахстан. При этом доля киберпреступлений в общей структуре зарегистрированных преступлений в России в два раза больше, чем в Казахстане. Однако одна из опасных тенденций киберпреступности в Казахстане заключается в значительно более высоких темпах роста киберпреступности, чем в России: за последние 8 лет они превысили темпы роста киберпреступности в России в три раза.

3. В структуре киберпреступности как в России, так и в Казахстане подавляющее большинство составляют преступления, совершаемые

с использованием информационно-телекоммуникационных технологий, среди которых в Российской Федерации 63,53% занимают киберпреступления против собственности, при этом наиболее распространенными видами являются мошенничество (около 50%) и кража (14%). В Республике Казахстан киберправонарушения против собственности составляют еще большую долю — 94,46%, но среди них наиболее распространено мошенничество (около 90% — мошенничество и 4% — кража).

В целом учитывая, что данные признаки носят устойчивый характер, определяют особенности состояния и структуры общей преступности в Российской Федерации и Республике Казахстан, наблюдаются в большинстве регионов, поэтому киберпреступность можно рассматривать как **один из основных видов национальной преступности**. При этом в ходе исследования нами определена тенденция к усилению роли искусственного интеллекта в информационно-телекоммуникационном воздействии преступников на граждан.

4. В целях дифференциации предупредительного воздействия на лиц, совершающих киберпреступления, предложена классификация киберпреступников, основанная на степени их вовлеченности в преступную деятельность:

1) начинающие киберпреступники (51,7%) характеризуются средним уровнем дохода и обладают способностью использовать одно или несколько компьютерных устройств. Их возраст колеблется от 18 до 30 лет, как правило, это мужчины с базовым образовательным уровнем (среднее, среднее специальное). Их профессиональная деятельность часто связана с информационными технологиями, хотя некоторые из них не имеют постоянной работы;

2) устойчивые киберпреступники (37,4%) достигли среднего или выше среднего уровня дохода и имеют углубленные знания в области информационных технологий. Их возрастная категория от 20 до 25 лет, преимущественно мужчины, хотя наблюдается тенденция к увеличению активности женщин (5%). Обычно они обладают высшим техническим образованием и способны использовать инновационные компьютерные системы;

3) профессиональные киберпреступники (10,9%) отличаются высоким уровнем материального благосостояния, находятся в возрасте от 25 лет до 49 лет. Среди них преобладают мужчины (женщины — 8%). Они имеют высшее техническое образование и высокий уровень профессиональных знаний в области информационных и сетевых технологий, постоянно совершенствуя свои навыки в использовании инструментов для совершения киберпреступлений, включая собственные разработки (6,8% из всех).

5. Выявлены характерные особенности личности российских киберпреступников, к которым относятся **кибермошенники и киберворы**. Это повышенный уровень корыстных устремлений в сочетании с отсутствием постоянного источника дохода при нормальной трудоспособности, значительный профессионализм в использовании ИТ-технологий для достижения преступных целей, отсутствие явного криминального прошлого, наличие определенного жизненного опыта, о чем свидетельствуют возраст от 30 до 49 лет и среднее профессиональное образование, наличие навыков психологического воздействия, выстраивания доброжелательных отношений с собеседниками. Лица, совершающие кибермошенничества в Казахстане, как правило, представлены мужчинами, гражданами Республики Казахстан, в возрасте от 21 года до 29 лет, имеющими среднее специальное образование, неработающими. Они в среднем на 15 лет младше, чем кибермошенники в Российской Федерации.

Особенностями лиц, совершающих киберпреступления в сфере компьютерной информации в России, являются: желание легкой наживы, преобладание индивидуализма при совершении киберпреступлений, отверженность к определенному способу, специализации в использовании ИТ-технологий при наличии многообразия способов совершения киберпреступлений. Их характеризуют также постоянное проживание в данной местности, молодой возраст от 18 до 24 лет, наличие среднего профессионального образования, работа в сфере информационных технологий. В Казахстане преступники, совершающие уголовные правонарушения в сфере информатизации и связи, — это чаще всего мужчины, граждане Республики Казахстан в возрасте от 21 года до 39 лет, имеющие среднее специальное образование, в большинстве своем (81% случаев) нигде не работающие.

6. В ходе исследования определены внутренние и внешние приоритетные детерминанты наиболее распространенных киберпреступлений, совершаемых в России и Казахстане, необходимые для эффективной организации мер предупреждения киберпреступности.

Внутренние детерминанты:

- социально-экономические: широкое использование информационно-коммуникационных технологий в обществе; использование некачественного программного обеспечения (нелицензионных программ); несоответствие между потребностями населения в информационных услугах и программном обеспечении и их недоступностью из-за низкого уровня жизни; монопольное положение разработчиков программного обеспечения;

- организационно-технические: нарушения и недостаточное соблюдение мер информационной безопасности; низкий уровень осведомленности о правилах использования интернет-ресурсов; неэффективная защита

информационных систем, уязвимость программного обеспечения; отсутствие эффективных механизмов контроля и обнаружения кибератак;

— организационно-правовые: недостаточное правовое урегулирование на национальном уровне вопросов кибербезопасности; отсутствие единства в понимании основных терминов, связанных с кибербезопасностью и его производных (киберпространство, киберзащита, кибератаки, кибернападение, киберпреступность и др.), затрудняющее разработку эффективного законодательства, регулирующего вопросы предупреждения киберпреступлений; отсутствие эффективной правовой защиты интересов пострадавших от кибермошенников;

— организационно-управленческие: отсутствие стратегического подхода к противодействию киберугрозам на уровне предприятий, учреждений и организаций; недостаточное внимание руководства предприятий, организаций и учреждений к проблеме информационной безопасности; отсутствие типовых и специальных программ профилактики имущественных киберпреступлений, низкая квалификация специалистов и сотрудников правоохранительных органов в области кибербезопасности.

Внешние детерминанты:

— организационно-технического характера: деятельность международных киберпреступных группировок и отдельных хакеров; распространение вредоносного программного обеспечения и технологий, разработанных в других странах;

— организационно-правового характера: недостатки международно-правового регулирования вопросов предупреждения киберпреступности; сложности в международном сотрудничестве в расследовании и раскрытии киберпреступлений.

К особенностям детерминант киберпреступлений в России следует отнести: наличие существенного влияния внешних факторов, связанных с применением зарубежных санкций, в том числе в сфере технического и программного компьютерного обеспечения; внутренних социально-экономических факторов, обусловленных масштабами страны, определяющими большие возможности киберпреступникам для выбора своих жертв. В Казахстане к особенностям детерминант киберпреступлений следует отнести преобладание внутренних факторов социально-экономического характера, связанных прежде всего с безработицей, особенно среди молодого населения.

7. В целях совершенствования правового обеспечения предупреждения киберпреступности в Российской Федерации и Республике Казахстан необходимо установление баланса регулирования вопросов кибербезопасности на международном, межгосударственном и национальном уровнях.

В целом для этого на международном уровне необходимо подписание нашими странами единой международной Конвенции ООН против киберпреступности. На межгосударственном уровне в условиях санкционного давления для России особенно актуально принятие единых нормативных актов дружественных стран. На национальном уровне для Казахстана актуально принятие постановления Верховного Суда Республики Казахстан, разъясняющего и обеспечивающего единообразное применение казахстанскими судами законодательства об ответственности за уголовные правонарушения в сфере компьютерной информации, а также иные преступления, совершенные с использованием электронных или информационно-телекоммуникационных сетей, включая сеть Интернет.

8. Учитывая внутренние и внешние детерминанты, негативную динамику и общественную опасность киберпреступности в Российской Федерации и Республике Казахстан, в рамках основных направлений совершенствования предупреждения киберпреступлений предложено классифицировать меры предупреждения киберпреступности на государственном и межгосударственном уровнях соответственно сферам действия этих детерминант.

I. Государственный уровень. Меры, направленные на нейтрализацию внутренних факторов, обуславливающих совершение киберпреступлений:

- социально-экономические: включение общества в процессы выявления киберпреступлений, совершенствование информационной культуры, сотрудничество с частными компаниями и обеспечение доступности лицензионного программного обеспечения, обновление цифровых моделей, отражающих различные аспекты киберпреступности; создание баз данных, содержащих информацию о передовых методах обнаружения, раскрытия и расследования данных преступлений, разработка инструментов для онлайн-обнаружения планируемых, осуществляемых и уже совершенных киберпреступлений, а также лиц, к ним причастных;

- организационно-технические: внедрение образовательных курсов и пользовательских соглашений для повышения осведомленности граждан; совершенствование системы защиты информации; усиление кибербезопасности критической инфраструктуры; создание специализированных подразделений по ее защите; постоянный мониторинг телекоммуникационных сетей; накопление экспертных знаний; совершенствование взаимодействия правоохранительных органов для борьбы с киберпреступлениями транснационного характера;

- организационно-управленческие: внедрение формализованных принципов стратегического противодействия киберугрозам, направленных на оптимизацию соответствующих ответных действий; создание специализированных подразделений для быстрого раскрытия и расследования имуще-

ственных киберпреступлений по типу «Киберпола» в Казахстане; разработка и реализация специальных программ профилактики киберпреступлений имущественного характера; организация профильного обучения и повышения квалификации сотрудников правоохранительных и судебных органов.

II. Межгосударственный уровень. Меры, направленные на сокращение внешних факторов, обуславливающих совершение киберпреступлений в Российской Федерации и Республике Казахстан:

- пресечение влияния недружественных государств;
- установление эффективного международного сотрудничества, позволяющего национальным правительствам следовать установленным нормам и правилам, не испытывая внешнего давления;
- обмен информацией об использовании российского и казахстанского опыта применения эффективных мер борьбы с киберпреступностью, адаптации международных методов выявления и изучения новых форм киберпреступлений, законодательных решений, касающихся обеспечения безопасности информационных сетей; участие в международных форумах, конференциях и совещаниях по выработке мер по координации действий, направленных на предотвращение киберугроз.

Степень достоверности и апробация результатов исследования определяются широким диапазоном методик и эмпирической базой, сформированной с учетом объекта и предмета исследования, включающей изучение:

- статистических данных ГИАЦ МВД России о преступлениях, совершаемых с использованием информационно-телекоммуникационных технологий и в сфере компьютерной информации, за период с 2016 г. по 2024 г.;
- статистических данных Комитета по правовой статистике и специальным учетам Генеральной прокуратуры Республики Казахстан об уголовных правонарушениях, совершаемых с использованием информационных технологий и в сфере информатизации и связи, за период с 2016 г. по 2024 г.;
- сведений в форме статистической отчетности Судебного департамента при Верховном Суде Российской Федерации «Отчет о демографических признаках осужденных по всем составам преступлений Уголовного кодекса Российской Федерации», а именно за преступления, совершаемые с использованием информационно-телекоммуникационных технологий и в сфере компьютерной информации, за период с 2021 г. по 2024 г.;
- данных отчета Комитета по правовой статистике и специальным учетам Генеральной прокуратуры Республики Казахстан о демографических признаках осужденных за преступления, совершаемые с использованием информационных технологий и в сфере информатизации и связи за период с 2021 г. по 2024 г.;

— 153 приговоров районных, городских и областных судов Омской, Новосибирской, Иркутской областей Российской Федерации, вынесенных за совершение преступлений с использованием информационно-телекоммуникационных технологий и в сфере компьютерной информации;

— 163 приговоров, вынесенных судами Актюбинской, Костанайской и Карагандинской областей Республики Казахстан за совершение преступлений с использованием информационных технологий и в сфере информатизации и связи;

— результатов анкетирования сотрудников правоохранительных органов Российской Федерации (268 респондентов) и Республики Казахстан (243 респондента);

— результатов анкетирования населения России (320 респондентов) и Казахстана (434 респондента).

Теоретические выводы, сформулированные в результате исследования, практические рекомендации и обобщенные статистические данные использовались для проведения учебных занятий с курсантами, слушателями, сотрудниками органов внутренних дел, проходящими повышение квалификации в Омской академии МВД России, Карагандинской академии МВД РК им. Б. Бейсенова, Костанайской академии МВД РК им. Ш. Кабылбаева; в процессе разработки учебных, учебно-методических материалов по учебным дисциплинам (модулям) «Криминология» и «Виктимология», в профессиональной деятельности органов внутренних дел.

Апробация и внедрение результатов исследования определены широким диапазоном научно-исследовательских работ, выполненных по следующим направлениям:

— диссертация обсуждалась и была одобрена на заседании кафедры криминологии и профилактики преступлений Омской академии МВД России;

— основные положения диссертационного исследования были обсуждены на 9 научно-практических конференциях и межвузовских семинарах, проведенных в Омской академии МВД России, Барнаульском юридическом институте МВД России, Сибирском юридическом институте МВД России (г. Красноярск), Сибирском юридическом университете (г. Омск), Карагандинской академии МВД РК им. Б. Бейсенова, Костанайской академии МВД РК им. Ш. Кабылбаева;

— аналитический обзор «Криминологическая характеристика киберпреступности в Российской Федерации и Республике Казахстан» внедрен в учебный процесс Карагандинской академии МВД РК им. Б. Бейсенова, Костанайской академии МВД РК им. Ш. Кабылбаева, Актюбинского юридического института МВД РК им. М. Букенбаева, Академии правосудия

при Верховном Суде Республики Казахстан, Барнаульского юридического института МВД России, Сибирского юридического института МВД России (г. Красноярск), в практическую деятельность Центра по борьбе с киберпреступностью Департамента криминальной полиции МВД РК, Управления дознания Департамента полиции Карагандинской области МВД РК, Управления полиции района «Сарыарка» Департамента полиции г. Астаны, Главного следственного управления Главного управления МВД России по Алтайскому краю, что подтверждается актами внедрения;

— основные результаты исследования нашли отражение в 15 научных публикациях общим объемом 4,94 п. л., 5 из которых размещены в рецензируемых научных изданиях, рекомендованных Высшей аттестационной комиссией при Минобрнауки России для опубликования основных научных результатов диссертаций.

Структура и объем работы обусловлены целями, задачами и логикой исследования. Диссертация состоит из введения, двух глав, объединяющих шесть параграфов, заключения, списка использованных источников и приложений. Объем работы соответствует требованиям Высшей аттестационной комиссии при Минобрнауки России.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обосновывается актуальность темы исследования, характеризуется степень ее разработанности; определяются объект, предмет, цель и задачи исследования; раскрываются ее теоретическая основа, научная новизна; аргументируется теоретическая и практическая значимость работы, указываются методология и методы исследования, формулируются положения, выносимые на защиту; приводятся сведения об апробации результатов исследования, а также о структуре и объеме работы.

Первая глава «Криминологическая характеристика киберпреступности в Российской Федерации и Республике Казахстан» состоит из трех параграфов.

В *первом параграфе* «Понятие и криминологическая природа киберпреступности» исследуются понятие и признаки киберпреступности, анализируются мнения ученых России и Казахстана по поводу ее содержания и основных признаков.

Автор отмечает, что понятие «киберпреступность» широко используется в криминологии и практической деятельности полиции в Российской Федерации и Республике Казахстан, однако вопрос о точном и полном понимании содержания киберпреступности, а также о его законодательном закреплении до сегодняшнего дня остается открытым.

Изучение и оценка определений киберпреступности, содержащихся в трудах ученых России и Казахстана, позволили выделить основные признаки киберпреступности:

- это преступность в информационном пространстве;
- объектом преступления являются информационная безопасность, собственность, авторское право, общественная безопасность, нравственность;
- охват всех преступных деяний, которые совершаются с использованием средств информационно-коммуникационных технологий;
- повышенная скрытность совершения преступления, которая обеспечена спецификой сетевого информационного пространства (развитые механизмы анонимности, сложность инфраструктуры и т. п.);
- возможность совершения преступления в автоматизированном режиме в нескольких местах одновременно;
- дистанционный характер преступных действий в условиях отсутствия физического контакта преступника и потерпевшего;
- очень высокий потенциал развития и нарастания неблагоприятных последствий, что приводит к дальнейшей невозможности предотвращения и пресечения преступлений данного вида традиционными средствами;
- несоответствие темпа роста преступной деятельности в киберпространстве темпам законодательного регулирования и реализации отдельных средств противодействия такой деятельности.

На основании вышеизложенного автором дается собственное определение киберпреступности.

Во *втором параграфе* «Состояние и тенденции киберпреступности» проведен сравнительный анализ структуры, динамики и тенденций киберпреступности в Российской Федерации и Республике Казахстан.

Диссертант обращает внимание на то, что в целом уровень, структура и динамика киберпреступности в Российской Федерации и Республике Казахстан имеют существенные отличия. Во-первых, отличие проявляется в доле киберпреступлений в общей массе преступности. Если в 2024 г. в России доля киберпреступлений в общей структуре зарегистрированных преступлений составляла 40,0%, то в Казахстане она была значительно меньше — 18,9%. Во-вторых, темпы роста киберпреступности. В 2016 г. в России доля киберпреступлений в общей структуре зарегистрированных преступлений занимала 4,2%, а к 2024 г. она увеличилась в 9,5 раза и составила 40,0%. В 2016 г. в Казахстане доля киберпреступлений в общей структуре зарегистрированных преступлений составляла 0,24%, а к 2024 г. она увеличилась в 79 раз и достигла 18,9%.

Отмечается, что киберпреступления (уголовные правонарушения в Казахстане) в сфере компьютерной информации на сегодняшний день

в структуре киберпреступности в Российской Федерации составляют 13,82% и в Республике Казахстан — 0,28%. В Российской Федерации наиболее распространенными видами киберпреступлений в структуре общей преступности являются мошенничество (49,69%), кража (13,84%), незаконные производство, сбыт или пересылка наркотических средств, психотропных веществ, а также незаконные сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества (12,37%).

В Республике Казахстан распространенным видом уголовных киберправонарушений в общей структуре общей преступности выступает мошенничество (89,97%). Соответствующую оценку состояния преступности в России и Казахстане дают и сотрудники правоохранительных органов этих стран. Так, по результатам проведенного диссертантом опроса 50,0% сотрудников правоохранительных органов Российской Федерации и 49,79% сотрудников правоохранительных органов Республики Казахстан оценивают уровень киберпреступности как высокий и до 20% их в каждой стране — как сверхвысокий. При этом 59,7% в России и 76,95% опрошенных в Казахстане считают, что общественная опасность киберпреступлений только возрастает. Более того, 29,85% респондентов в России и 40,32% в Казахстане отметили, что нынешнее состояние киберпреступности угрожает безопасности их стран.

Определены предполагаемые направления развития киберпреступности с использованием искусственного интеллекта, которые включают облегчение доступа в эту сферу для лиц с ограниченными техническими знаниями, позволяя им осуществлять кибератаки и организовывать сложные схемы мошенничества.

В *третьем параграфе* «Особенности лиц, совершающих киберпреступления» проведен анализ наиболее значимых социально-демографических, нравственно-психологических, уголовно-правовых качеств киберпреступников.

Представленные в работе сведения свидетельствуют о том, что кибермошенниками являются лица более старшего возраста, чем лица, привлекаемые к ответственности за киберпреступления в сфере компьютерной информации. В среднем это трудоспособные, без постоянного источника дохода, постоянные жители данной местности в возрасте от 30 до 49 лет, имеющие высшее профессиональное, среднее профессиональное, среднее общее образование.

Среди киберпреступников наблюдается преобладание представителей молодого поколения, так как навыки владения компьютером закладываются в более раннем, дошкольном возрасте. Немаловажное значение в формировании личности хакера также имеют уровень образования и социальное

положение. Так, среди киберпреступников в Республике Казахстан доля лиц со средним и средним специальным образованием составляет 76,4%, с высшим образованием — 20,0%. На долю безработных приходится 82,3%, отсюда следует, что преступления в основном совершаются лицами с низким уровнем доходов либо не имеющими вообще никаких доходов. Ранее судимыми лицами совершено 36,4% киберпреступлений. Часто киберпреступления совершаются в составе организованной преступной группы.

На основании проведенного исследования предложена классификация лиц, занимающихся киберпреступлениями, основанная на степени их вовлеченности в преступную деятельность.

Вторая глава «Детерминация и предупреждение киберпреступности в Российской Федерации и Республике Казахстан» состоит из трех параграфов.

В первом параграфе «Детерминанты киберпреступности» выделяются объективные и субъективные причины и условия, а также иные факторы, определяющие детерминацию киберпреступности в России и Казахстане.

Исходя из целей и задач исследования, предлагается выделять две группы основных детерминант киберпреступности в Российской Федерации и Республике Казахстан: внутренние и внешние. При этом в каждой из основных групп детерминант выделены подгруппы детерминант, отражающие специфику действия факторов, обуславливающих совершение киберпреступлений, связанных с основными сферами жизнедеятельности общества и способами их влияния на общество: социально-экономические, организационно-технические, правовые, организационно-управленческие.

Социально-экономические детерминанты, по мнению автора, связаны с широким использованием информационно-коммуникационных технологий в обществе, а также сосредоточением в сети Интернет большого количества персональных данных граждан наших стран. Отмечается, что основные условия роста киберпреступности в Российской Федерации и Республике Казахстан — это цифровизация финансовых услуг, расширение электронной коммерции, смена потребительских привычек на фоне пандемии COVID-19, а также стремительная эволюция киберпреступности.

По итогам анкетирования населения Российской Федерации и Республики Казахстан диссертантом выявлено, что 78,80% респондентов столкнулись с фактом интернет-мошенничества.

К организационно-техническим детерминантам автор относит низкий уровень осведомленности о правилах использования интернет-ресурсов, недостаточное внимание руководства организаций к проблеме информационной безопасности, некомпетентность и невысокую квалификацию специалистов организации и сотрудников правоохранительных органов в области

кибербезопасности, несовершенную защиту информационных систем, уязвимость программного обеспечения, отсутствие эффективных механизмов контроля и обнаружения кибератак.

Что касается организационно-правовых детерминант, то отмечено, что одним из главных факторов, способствующих развитию киберпреступности, является недостаточное законодательное регулирование, которое на самом деле должно быть направлено на предотвращение и противодействие киберпреступлениям, но, к сожалению, оно не обеспечивает надлежащей защиты граждан от таких преступлений.

По мнению диссертанта, организационно-управленческие детерминанты связаны с недостатками в стратегии и тактике организации предупреждения киберпреступлений на общем и региональном уровнях, отсутствием стратегического подхода к противодействию киберугрозам на уровне предприятий, учреждений и организаций. Недостаток четкой и эффективной стратегии кибербезопасности в организациях приводит к нескоординированным и неполным мерам безопасности, оставляющим уязвимости, которыми пользуются киберпреступники.

Диссертантом выделяются и внешние детерминанты, связанные как с активными действиями недружественных государств по нарушению нормального развития наших государств, так и с отсутствием должного взаимодействия между государствами в борьбе с киберпреступностью, вследствие чего появляются условия для совершения киберпреступлений.

Во *втором параграфе* «Правовое обеспечение предупреждения киберпреступности» рассмотрено содержание совокупности нормативных правовых актов, принимаемых на различных уровнях власти в целях борьбы с киберпреступностью.

Отмечено, что для формирования эффективной национальной системы нормативных правовых актов конкретных государств по предупреждению киберпреступности, отражающей комплексные права и обязанности государств по вопросам кибербезопасности, все существующие нормативные правовые акты необходимо формировать иерархично на следующих уровнях:

- 1) акты всемирного уровня;
- 2) акты межнационального уровня;
- 3) акты отдельных государств (национальное законодательство).

Предлагается в группе международно-правовых актов Организации Объединенных Наций по обеспечению кибербезопасности (информационной безопасности) и сотрудничеству в борьбе с киберпреступностью в качестве первоочередных мер разработать единый подход к определению киберпреступности.

Анализ позиций ученых, международных актов и нормативных правовых актов Российской Федерации и Республики Казахстан, направленных на обеспечение кибербезопасности и борьбу с киберпреступностью, позволил автору сформулировать следующие выводы:

- отсутствует единая система нормативных правовых актов в России и Казахстане, направленных на предотвращение киберпреступности. Создание подобной системы возможно только на основании правового регулирования, охватывающего три уровня: мировой, региональный и национальный;

- для систематизации государственной политики Российской Федерации в области кибербезопасности необходимо разработать концепцию кибербезопасности России, используя соответствующий опыт Республики Казахстан;

- для общепризнанного законодательного определения термин «кибербезопасность» и его производные (киберпространство, киберзащита, кибератаки, кибернападение, киберпреступность и др.) необходимо закрепить на международном уровне;

- уполномоченным подразделениям органов внутренних дел необходимо проводить систематический мониторинг способов совершения киберпреступлений в целях постоянного совершенствования законодательства, учитывая быстрое развитие средств и методов совершения таких преступлений.

Наиболее продуктивной представляется ориентация на развитие законодательства о профилактике и противодействии киберпреступности на уровне стран СНГ на основе директивных документов этого содружества. В целях совершенствования правового обеспечения предупреждения киберпреступности в Российской Федерации и Республике Казахстан необходимо достижение баланса регулирования вопросов кибербезопасности на международном, межгосударственном и национальном уровнях.

На межгосударственном уровне в условиях санкционного давления для России особенно актуально принятие единых нормативных актов дружественных для России стран. На национальном уровне для Казахстана актуально принятие нормативного постановления Верховного Суда Республики Казахстан, разъясняющего и обеспечивающего единообразное применение казахстанскими судами законодательства об уголовной ответственности за уголовные правонарушения в сфере компьютерной информации, а также иные преступления, совершенные с использованием электронных или информационно-телекоммуникационных сетей, включая сеть Интернет.

В *третьем параграфе* «Меры предупреждения киберпреступлений» проводится анализ мер, направленных на нейтрализацию действия выяв-

ленных детерминант киберпреступности в России и Казахстане, и вносятся предложения по повышению их эффективности.

Среди мер предупреждения киберпреступности, ориентированных на устранение внутренних факторов, определяющих ее существование в современном виде в России и Казахстане, выделяются прежде всего социально-экономические меры предупреждения киберпреступности: проведение системной политики кибербезопасности, взаимоувязывающей все ее направления, такие как защита персональных данных граждан и критическая информационная инфраструктура; проведение кампаний, направленных на повышение компетентности и образования в целях совершенствования информационной грамотности и осознания потенциальных угроз в интернете, что включает осведомление пользователей о методах обнаружения и предотвращения кибератак, защите личных данных и информации, а также сочетание виктимологической профилактики и разработки личных стратегий защиты личной информации в сети; создание механизма обеспечения доступности населению лицензионного программного обеспечения; устранение негативных последствий в экономической сфере Российской Федерации с помощью эффективной государственной поддержки малого и среднего бизнеса, а также замещения импортных товаров отечественными. В рамках организационно-технических мер предупреждения киберпреступности автор выделяет меры, связанные с разработкой, внедрением, непосредственной реализацией и усовершенствованием технических мер, направленных на обеспечение безопасности в сфере информации и информационных технологий, в том числе создание материально-технической базы для подразделений, занимающихся противодействием киберпреступности, основанной на современных высоких технологиях, снижение уязвимостей в информационных системах, а также иное техническое содействие развитию сектора кибербезопасности.

В рамках организационно-управленческих мер предупреждения киберпреступности выделяется необходимость внедрения формализованных принципов стратегического противодействия киберугрозам, ориентированных на оптимизацию соответствующих ответных действий; создание специализированных подразделений для быстрого раскрытия и расследования имущественных киберпреступлений по типу «Киберпола» в Казахстане; разработку и реализацию специальных программ профилактики киберпреступлений имущественного характера; своевременное повышение квалификации и профильное обучение сотрудников правоохранительных органов, занимающихся раскрытием и расследованием киберпреступлений имущественной направленности, приемам и способам разработки и применения актуальных мер предупреждения данных преступлений.

Среди мер предупреждения киберпреступности также выделяются меры, ориентированные на устранение внешних факторов, определяющих ее существование в современном виде в России и Казахстане, при этом особое внимание акцентируется на ограничительных мерах, связанных с пресечением негативного влияния на наши страны деятельности недружественных государств, прежде всего, с нейтрализацией деятельности киберпреступных группировок и хакеров, которые используют свои навыки и ресурсы для совершения киберпреступлений, а также с противодействием установленным против России санкциям в различных сферах деятельности нашего государства.

Важным направлением предупреждения киберпреступлений имущественного характера является работа по блокировке исходящих из недружественных стран ближнего и дальнего зарубежья звонков в рамках интернет-мошенничества, связанного с оформлением на граждан кредитов и займов, а также хищением их банковских накоплений. Необходимо распространять и использовать опыт правоохранительных органов Казахстана, которые на сегодняшний день успешно внедряют систему блокировки «зарубежных» звонков с подменных номеров, используемых мошенниками. Это позволило пресечь свыше 43 млн попыток таких соединений, вследствие чего количество пострадавших сократилось более чем в 2,5 раза.

Противодействие использованию вредоносного программного обеспечения и технологий из других стран направлено, прежде всего, на разработку в России и Казахстане собственного программного обеспечения и своих информационных технологий.

К особенностям предупреждения киберпреступлений в России, по мнению диссертанта, следует отнести принятие мер, направленных на нейтрализацию влияния внешних факторов, связанных с применением зарубежных санкций, путем разработки собственного технического и программного компьютерного обеспечения. В Казахстане к особенностям предупреждения киберпреступлений следует отнести принятие мер, направленных на снижение уровня безработицы среди молодого населения.

В **заключении** излагаются основные выводы и предложения, сформулированные в ходе диссертационного исследования, а также перспективы дальнейшей разработки темы.

В **приложениях** содержатся результаты проведенного автором анкетирования сотрудников правоохранительных органов и населения, а также результаты анализа приговоров судов России и Казахстана.

**Основные положения диссертационного исследования
опубликованы в следующих работах:**

Статьи в рецензируемых научных изданиях, рекомендованных Высшей аттестационной комиссией при Министерстве науки и высшего образования Российской Федерации для опубликования основных научных результатов диссертаций:

1. Карабеков, К. О. Понятие киберпреступности в Российской Федерации и Республике Казахстан / К. О. Карабеков. — Текст : непосредственный // Известия Юго-Западного государственного университета. Серия : История и право. — 2022. — Т. 12, № 5. — С. 94–102 (0,69 п. л.).

2. Карабеков, К. О. Правовое обеспечение предупреждения киберпреступности в Российской Федерации и Республике Казахстан / К. О. Карабеков. — Текст : непосредственный // Известия Юго-Западного государственного университета. Серия : История и право. — 2023. — Т. 13, № 3. — С. 156–168 (0,92 п. л.).

3. Карабеков, К. О. Криминологическая характеристика личности киберпреступника в Российской Федерации и Республике Казахстан / В. В. Бабурин, К. О. Карабеков. — Текст : непосредственный // Психопедагогика в правоохранительных органах. — 2024. — Т. 29, № 1. — С. 113–119 (0,45 п. л. / 0,45 п. л.).

4. Карабеков, К. О. Состояние и тенденции киберпреступности в Российской Федерации и Республике Казахстан / К. О. Карабеков. — Текст : непосредственный // Научный вестник Омской академии МВД России. — 2024. — Т. 30, № 2. — С. 106–112 (0,58 п. л.).

5. Карабеков, К. О. Детерминанты и меры предупреждения киберпреступлений в Российской Федерации и Республике Казахстан / К. О. Карабеков. — Текст : непосредственный // Евразийский юридический журнал. — 2025. — № 7. — С. 356–357 (0,34 п. л.).

Иные публикации:

6. Карабеков, К. О. Актуальные вопросы исследования киберпреступности в Российской Федерации и Республике Казахстан / К. О. Карабеков. — Текст: непосредственный // Актуальные проблемы борьбы с преступлениями и иными правонарушениями : материалы XX международной научно-практической конференции : в 2 частях. — Барнаул : Барнаульский юридический институт МВД России, 2022. — Часть 2. — С. 25–27 (0,14 п. л.).

7. Карабеков, К. О. Некоторые вопросы профилактики киберпреступности в молодежной среде / К. О. Карабеков. — Текст : непосредственный // Противодействие наркоугрозе на современном этапе : правовой и социально-

гуманитарный аспекты : материалы международного научно-практического семинара. — Красноярск : Сибирский юридический институт МВД России, 2022. — С. 96–99 (0,18 п. л.).

8. *Карабеков, К. О.* Роль кибердружин в противодействии интернет-угрозам / К. О. Карабеков. — Текст : непосредственный // Современные тенденции развития юридической науки : материалы международной научно-теоретической конференции молодых ученых, посвященной Дню казахстанской науки. — Караганда : Карагандинская академия МВД Республики Казахстан им. Б. Бейсенова, 2022. — С. 36–38 (0,18 п. л.).

9. *Карабеков, К. О.* Некоторые вопросы борьбы с киберпреступностью в России / К. О. Карабеков. — Текст : непосредственный // Проблемы и перспективы совершенствования законодательства и правоприменительной практики органов внутренних дел : материалы международной научно-практической конференции, посвященной 30-летию казахстанской полиции. — Караганда : Карагандинская академия МВД Республики Казахстан им. Б. Бейсенова, 2022. — С. 98–102 (0,23 п. л.).

10. *Карабеков, К. О.* Профилактика кибербуллинга в подростковой среде / К. О. Карабеков. — Текст : непосредственный // Защита прав детей: сотрудничество полиции и гражданского общества : материалы международной научно-практической конференции. — Костанай : Костанайская академия МВД Республики Казахстан имени Шракбека Кабылбаева, 2022. — С. 71–76 (0,26 п. л.).

11. *Карабеков, К. О.* Опыт Республики Казахстан по борьбе с киберпреступностью / К. О. Карабеков. — Текст : непосредственный // Преемственность и новации в юридической науке : материалы всероссийской научной конференции адъюнктов, аспирантов и соискателей. — Омск : Омская академия МВД России, 2022. — Вып. 18. — С. 58–59 (0,18 п. л.).

12. *Карабеков, К. О.* Причины и условия киберпреступности в Республике Казахстан / К. О. Карабеков. — Текст: электронный // Актуальные проблемы профилактики преступлений : материалы международного научно-практического семинара. — Омск : Омская академия МВД России, 2023. — С. 47–50 (0,23 п. л.).

13. *Карабеков, К. О.* Проблемы предупреждения киберпреступлений в Республике Казахстан / К. О. Карабеков. — Текст : непосредственный // Актуальные проблемы уголовной и уголовно-процессуальной политики Российской Федерации : материалы международной научно-практической конференции. — Омск : Сибирский юридический университет, 2023. — С. 118–122 (0,20 п. л.).

14. *Карабеков, К. О.* Актуальность использования возможностей нейросетей в предупреждении преступности / К. О. Карабеков. — Текст :

непосредственный // Преемственность и новации в юридической науке : материалы международной научной конференции адъюнктов, аспирантов и соискателей. — Омск : Омская академия МВД России, 2023. — Вып. 19. — С. 50–52 (0,18 п. л.).

15. *Карабеков, К. О.* Основные направления совершенствования мер предупреждения интернет-мошенничества в Республике Казахстан / К. О. Карабеков. — Текст : непосредственный // Преемственность и новации в юридической науке : материалы международной научной конференции адъюнктов, аспирантов и соискателей. — Омск : Омская академия МВД России, 2024. — Вып. 20. — С. 57–59 (0,18 п. л.).

Подписано в печать ____ .10.2025

Усл. печ. л. 1,5
Тираж 130 экз.

Уч.-изд. л. 1,5
Заказ № ____

ОПиОП РИО Омской академии МВД России
644092, г. Омск, пр-т Комарова, д. 7