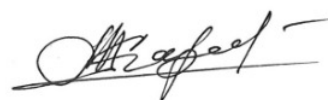


Федеральное государственное казенное образовательное учреждение
высшего образования
«Омская академия Министерства внутренних дел Российской Федерации»

На правах рукописи



Карабеков Канатбек Омирзакович

**КИБЕРПРЕСТУПНОСТЬ В РОССИЙСКОЙ ФЕДЕРАЦИИ
И РЕСПУБЛИКЕ КАЗАХСТАН: СОСТОЯНИЕ И МЕРЫ
ПРЕДУПРЕЖДЕНИЯ**

Специальность 5.1.4. Уголовно-правовые науки

ДИССЕРТАЦИЯ

на соискание ученой степени

кандидата юридических наук

Научный руководитель:
Заслуженный работник высшей школы
Российской Федерации,
доктор юридических наук,
профессор
Бабурин Василий Васильевич

Омск 2025

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ	3
ГЛАВА 1. КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА КИБЕРПРЕСТУПНОСТИ В РОССИЙСКОЙ ФЕДЕРАЦИИ И РЕСПУБЛИКЕ КАЗАХСТАН.....	20
§ 1. Понятие и криминологическая природа киберпреступности.....	20
§ 2. Состояние и тенденции киберпреступности	33
§ 3. Особенности лиц, совершающих киберпреступления	51
ГЛАВА 2. ДЕТЕРМИНАЦИЯ И ПРЕДУПРЕЖДЕНИЕ КИБЕРПРЕСТУПНОСТИ В РОССИЙСКОЙ ФЕДЕРАЦИИ И РЕСПУБЛИКЕ КАЗАХСТАН.....	70
§ 1. Детерминанты киберпреступности	70
§ 2. Правовое обеспечение предупреждения киберпреступности	103
§ 3. Меры предупреждения киберпреступлений	129
ЗАКЛЮЧЕНИЕ	154
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ.....	164
ПРИЛОЖЕНИЯ.....	199

ВВЕДЕНИЕ

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 правоохранительные 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, без-

опасности 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 киберпространстве 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 обуславливается 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, кибер-

мошенничества 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 обуславливается 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. Прозументова, 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. Рустемова, 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 ме-

ры борьбы» (Владивосток, 2005); Т. М. Лопатиной «Криминологические и уголовно-правовые основы противодействия компьютерной преступности» (Москва, 2006); А. К. Нурпеисовой «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 осо-

бенностей 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 киберпреступников 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 правоохрнительными органами России и Казахстана для своевременного прогнозирования состояния киберпреступности в данных странах, выявления и предупреждения киберпреступлений, прежде всего корыстной направленности; в законотворческой 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 киберпреступности, 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 ла-

тентностью 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, приверженность 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 преду-

преждения 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 трансграничного характера;

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

ГЛАВА 1. КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА КИБЕРПРЕСТУПНОСТИ В РОССИЙСКОЙ ФЕДЕРАЦИИ И РЕСПУБЛИКЕ КАЗАХСТАН

§ 1. Понятие и криминологическая природа киберпреступности

Увеличение числа преступных деяний, совершаемых с использованием сети Интернет, позволяет ученым говорить о сформировавшемся феномене киберпреступности, что вызывает необходимость его криминологического изучения¹.

В современном обществе инновационные технологии развиваются постоянно, люди активно пользуются возможностями сети Интернет, которая представлена в качестве децентрализованной мировой системы многоаспектных информационно-телекоммуникационных сетей и характеризуется специальным назначением по целевой трансляции информации посредством вычислительной техники и современной связи². Постоянная работа по модернизации информационного пространства предшествует криминализации информационной среды, и, как следствие, преступность виртуализируется и динамично перемещается в киберпространство³.

В настоящее время в законодательстве Российской Федерации и Республики Казахстан не сформулированы юридико-технические подходы к пониманию терминов «компьютерная преступность», «киберпреступность».

Первые упоминания об указанных терминах появились в прессе США, и такие преступления интерпретировались как связанные с ЭВМ. Позднее под ними стали понимать противоправные или неэтичные действия, связанные с автоматизированной обработкой данных в информационных системах.

¹ *Карабеков К. О.* Актуальные вопросы исследования киберпреступности в Российской Федерации и Республике Казахстан // Актуальные проблемы борьбы с преступлениями и иными правонарушениями : мат-лы XX междунар. науч.-практ. конф. : в 2 ч. Барнаул, 2022. Ч. 2. С. 27.

² *Джансараева Р. Е.* Борьба с киберпреступлениями: сравнительный анализ законодательства стран СНГ // Криминологический журнал Байкальского государственного университета экономики и права. 2012. № 3. С. 96.

³ *Рассолов И. М.* Право и Интернет. Теоретические проблемы. М., 2003. С. 134.

Новый этап роста компьютерной преступности начался с использования электронных банковских расчетов, чему способствовало быстрое развитие локальных и глобальных сетей.

Появились компьютерные преступники, специализирующиеся на проникновении в отдаленные информационные системы¹.

Известным компьютерным преступником является Кевин Митник, программист из Лос-Анжелеса, который 17-летним мальчиком был задержан за кражу списка паролей доступа у американской телефонной компании PacificBell. Широкую известность получила его война с Digital Equipment, которая в 1995 г. была проиграна Тсутому Шимомури, специалисту по безопасности компьютерных систем. Сумма убытка, причиненного хакером, составила несколько десятков миллионов долларов. 21 января 2000 г. Кевина выпустили из тюрьмы, запретив пользоваться не только компьютерами, но и любыми цифровыми устройствами, включая телефон².

Самый известный из постсоветских хакеров Владимир Левин перехитрил систему безопасности американского банка Citibank и с помощью удаленного доступа похитил около 12 млн долларов США, за что в дальнейшем был осужден за несанкционированный доступ в локальную сеть Банка промышленности Китая³.

В Казахстане вопрос о законодательном закреплении компьютерных преступлений в качестве самостоятельного уголовно наказуемого деяния впервые был поставлен при подготовке проекта Уголовного кодекса в конце 1995 г., и в 1997 г. в уголовное законодательство была включена ст. 227 «Неправомерный доступ к компьютерной информации, создание, использование и распространение вредоносных программ для ЭВМ»⁴.

В России осмысление феномена киберпреступности как неизвестной ранее формы уголовно наказуемых деяний началось с положений Уголовного кодекса

¹ История появления киберпреступности. URL: <https://www.cibercriminals.ru/crimenal/> (дата обращения: 18.11.2023).

² Там же.

³ Там же.

⁴ Нурпеисова А. К. Уголовно-правовые и криминалистические аспекты компьютерной преступности : автореф. дис. ... канд. юрид. наук. Караганда, 2010. С. 4.

1996 г. Структура уголовно-правовых норм стала развиваться на стыке понимания информационных и компьютерных преступлений¹.

В России насчитывается 127,6 млн интернет-пользователей, т. е. 88,2% общей численности населения в стране². В Казахстане количество абонентов сотовой связи, имеющих доступ к интернету, составляет 17,4 млн (87%)³. Объясняется это тем, что интернет-пространство на сегодняшний день является неотъемлемой частью жизни каждого человека, поскольку все социально значимые сферы жизнедеятельности, в частности работа, учеба и коммуникации, плавно перетекают в киберпространство.

Повышение роли киберпространства как интерактивной информационно-коммуникационной среды влечет за собой появление целого комплекса новых рисков и угроз, рост уязвимости информационной инфраструктуры, увеличение способов деструктивного воздействия на общественные отношения с использованием возможностей киберпространства. Их постоянная модификация чаще всего происходит в целях совершения преступлений⁴.

В начале 60-х гг. XX в. понятие и основные признаки киберпреступлений были определены термином «преступления, связанные с компьютерами»⁵. В 1979 г. термин «*cybercrime*» стали понимать как «использование или попытка использования компьютера, вычислительной системы или сети компьютеров с целью получения денег, собственности или услуг, обманывая либо выдавая себя за другое лицо; несанкционированное действие, имеющее целью уничтожение, изменение, повреждение или похищение вычислительной системы, компьютера,

¹ Пучков Д. В. Состояние уголовно-правового регулирования киберпреступлений в уголовном законодательстве Российской Федерации // Правовая политика и правовая жизнь. 2019. № 1. С. 65.

² Отчет DataReportal: цифровизация России в 2023 году. URL: <https://drozd.red/blog/marketing/otchet/> (дата обращения: 18.11.2023).

³ В Казахстане активно растет количество пользователей интернета. URL: <https://ranking.kz/digest/industries-digest/> (дата обращения: 18.11.2023).

⁴ Сидорова Е. З. Современный понятийный аппарат киберпреступности // Вестник Тюменского института повышения квалификации сотрудников МВД России. 2024. № 1(22). С. 65.

⁵ Козлов В. Е. «Computer Crime»: что стоит за названием? // Центр исследования компьютерной преступности. URL: <http://www.crime-research.ru/library/CCrime.html> (дата обращения: 18.11.2023).

их сети или находящихся в них программ или информации; преднамеренное не-санкционированное нарушение связи между компьютерами, вычислительными системами или сетями компьютеров»¹.

Согласно рекомендациям экспертов ООН, термин «киберпреступность» охватывает любое преступление, которое может совершаться с помощью компьютерной системы или сети, в рамках компьютерной системы или сети или против компьютерной системы или сети². При таком подходе киберпреступлением можно считать любое преступление, совершенное в киберпространстве.

Понятие «киберпреступность» законодателем используется, но его определение не раскрывается ни в одном нормативном правовом акте. Представляется, что подобный законодательный пробел требует обязательного устранения с соответствующей ссылкой на обращение к нормативным документам³.

В некоторых иностранных законодательных актах термин «киберпреступность» официально закреплён в названии или содержании правовых норм, в частности, встречаются такие аналогичные понятия, как «компьютерные преступления», «информационные технологии», «электронные средства связи» и др.

В большинстве законодательных актов само содержание дефиниции не раскрывается, а лишь определяется круг преступных деяний, которые входят в понятие киберпреступности, – умышленное воздействие на компьютерные системы и данные или неправомерный доступ к компьютерной информации, охраняемой законом⁴.

В редких случаях в зарубежном законодательстве термин «киберпреступность» используется в качестве названия законодательного акта или его раздела, однако его толкования не содержится. В законодательстве государств, таких как

¹ Степанов-Егиянц В. Г. Методологическое и законодательное обеспечение безопасности компьютерной информации в Российской Федерации (уголовно-правовой аспект) : дис. ... д-ра юрид. наук. М., 2016. С. 42.

² Доклад X Конгресса ООН по предупреждению преступности и обращению с правонарушителями. URL: https://www.unodc.org/documents/congress/Networks_R.pdf (дата обращения: 18.02.2025).

³ Бородкина Т. Н., Павлюк А. В. Киберпреступления: понятие, содержание и меры противодействия // Социально-политические науки. 2018. № 1. С. 135–137.

⁴ Основные виды киберпреступности. Модуль 2. ООН. Вена, 2019. С. 5.

Султанат Оман и Республика Филиппины, данный термин является легальным, а его определение в нормативных правовых актах отсутствует¹.

Изучив международные правовые документы, регулирующие отношения государств в рамках противодействия киберпреступности, можно отметить, что лишь в немногих из них используется понятие киберпреступности. В актах, имеющих ключевое значение по указанному вопросу, понятие киберпреступности вообще отсутствует.

В Конвенции Совета Европы о компьютерных преступлениях 2001 г.², Конвенции Африканского союза о кибербезопасности 2014 г.³, в Соглашении о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации (Минск, 2001 г.)⁴ употребляется понятие «преступления в сфере компьютерной информации», определяемое как «уголовно наказуемое деяние, предметом посягательства которого является компьютерная информация»⁵.

В Соглашении между правительствами государств – членов Шанхайской организации о сотрудничестве 2011 г.⁶ «информационная преступность» опреде-

¹ Кучерков И. А. О понятии «киберпреступление» в законодательстве и научной доктрине // Юридическая наука. 2019. № 10. С. 78–81.

² Конвенция о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23 ноября 2001 г.) : с изменениями от 28 января 2003 г. Доступ из справ.-правовой системы «Гарант».

³ Конвенция Африканского союза о кибербезопасности и защите персональных данных 2014 г. URL: <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection> (дата обращения: 17.03.2023).

⁴ Соглашение о сотрудничестве государств – участников Содружества Независимых Государств с преступлениями в сфере компьютерной информации (Минск, 1 июня 2001 г.) // Собрание законодательства Российской Федерации. 2009. № 13, ст. 1460.

⁵ Чернякова А. В. Международный и зарубежный опыт уголовно-правового противодействия хищениям, совершаемым с использованием компьютерной информации // Юридическая наука и правоохранительная практика. 2018. № 4(46). С. 170.

⁶ Об утверждении Соглашения между правительствами государств – членов Шанхайской организации о сотрудничестве в области обеспечения международной информационной безопасности : распоряжение Правительства Российской Федерации от 16 июля 2009 г. № 984-р // Собрание законодательства Российской Федерации. 2009. № 30, ст. 3879.

ляется как «использование ресурсов и (или) воздействие на них в информационном пространстве в противоправных целях»¹.

Акты зарубежного законодательства не раскрывают содержания термина «киберпреступность», даже в случае его употребления. Международный союз электросвязи (International Telecommunication Union) придерживается мнения, что отсутствует необходимость рассмотрения понятия «киберпреступность» как правового термина².

Представляется, что, по мнению зарубежного законодателя, «киберпреступность» понимается только как совокупность противоправных деяний, направленных против конфиденциальности, доступности и защищенности компьютерных систем и данных.

Понятие «киберпреступность» широко используется учеными-криминологами Российской Федерации и Республики Казахстан. При этом вопрос о точном и полном понимании указанного термина, а также о его законодательном закреплении до сегодняшнего дня остается открытым. Сущность указанной проблемы заключается в том, что от правильного понимания киберпреступности зависит эффективность работы правоохранительных органов по предупреждению такого рода преступлений. Сейчас, в период бурного развития информационных технологий, количество преступлений, совершаемых в киберпространстве, растет пропорционально числу пользователей компьютерных сетей.

С течением времени это не теряет своей актуальности, более того, приобретает новые аспекты. Во-первых, способы совершения киберпреступлений быстро развиваются, соответственно, свойства киберпреступности тоже меняются; во-вторых, регулярно возникают новые киберугрозы для безопасности населения; в-третьих, темпы законодательного регулирования, предупредительная, профилактическая деятельность правоохранительных органов не успевают за темпом роста преступной деятельности в киберпространстве; в-четвертых, назрела потребность прогнозирования киберпреступности; в-пятых, появляется необходимость разра-

¹ *Талипова Л. Р.* Международно-правовая регламентация киберпреступности // Гуманитарные, социально-экономические и общественные науки. 2016. № 4. С. 121.

² *Кучерков И. А.* Указ. соч.

ботки адекватных мер предупреждения с использованием искусственного интеллекта.

В настоящее время темы борьбы с компьютерной преступностью и обеспечения кибербезопасности пользуются научной популярностью во всем мире: в учебных заведениях вводятся новые академические дисциплины, рассматривающие вопросы кибербезопасности, исследованиями киберпреступности занимаются ведущие специалисты разных направлений научного сообщества, но больше всего работники ИТ-сферы и юристы.

Обратимся к анализу понятия «киберпреступность».

1. По А. В. Федорову, киберпреступность – это преступность в информационном пространстве, моделируемом при помощи компьютера, в котором находятся сведения о лицах, предметах, фактах, событиях, явлениях и процессах, представленных в математическом, символьном или в любом другом выражении и находящихся в движении по локальным и глобальным компьютерным сетям, либо сведения, хранящиеся в памяти любого физического или виртуального устройства, а также другого носителя, специально предназначенного для их хранения, обработки и передачи¹.

2. По В. А. Номоконову, киберпреступность охватывает как преступность, в которой компьютер является предметом, а информационная безопасность – объектом преступления, так и иные деяния, где компьютеры используются как орудия или средства совершения преступлений против собственности, авторских прав, общественной безопасности или нравственности².

3. По мнению Т. Л. Тропиной, киберпреступность образуют деяния, совершенные в киберпространстве, представляющие собой виновные противоправные вмешательства в функционирование компьютеров, компьютерных программ, компьютерных сетей; несанкционированные модификации компьютерных дан-

¹ Федоров А. В. Информационная безопасность в мировом политическом процессе : учеб. пособие. М., 2006. С. 111.

² Номоконов В. А. Актуальные проблемы борьбы с киберпреступностью // Информационные технологии и безопасность : сб. науч. тр. междунар. конф. Киев, 2003. Вып. 3. С. 105.

ных, а также иные противоправные общественно опасные действия, совершенные с помощью или посредством компьютеров, компьютерных сетей и программ¹.

Вышеуказанные ученые (А. В. Федоров, В. А. Номоконов, Т. Л. Тропина), на наш взгляд, в своих определениях не раскрывают все признаки киберпреступности, делая акцент на предмете киберпреступления и обобщая киберпреступность как преступность в информационном пространстве или киберпространстве.

4. С точки зрения И. Г. Чекунова, киберпреступность – это самостоятельный вид преступности, который определяется посредством применения признаков объективной стороны, таких как средство совершения преступления и орудие совершения преступления. В качестве них выступают вредоносная программа или техническое средство, подключенное к сети Интернет, использование которого направлено на причинение ущерба физическому или юридическому лицу. На его взгляд, понятие «киберпреступность» охватывает все преступные деяния, которые совершаются с использованием средств информационно-коммуникационных технологий². Полагаем, что этот автор шире охватывает понятие киберпреступности в современных реалиях, учитывая совершение киберпреступлений с использованием средств информационно-коммуникационных технологий.

5. По Т. Н. Шарыповой и А. А. Сидоренко, киберпреступность сочетает в себе «любое преступление, которое может совершаться с помощью компьютерной системы или сети, в рамках компьютерной системы или сети, против компьютерной системы или сети»³ (но при этом они не учитывают использования других средств информационно-коммуникационных технологий, например различ-

¹ Тропина Т. Л. Киберпреступность и кибертерроризм // Организованная преступность, терроризм и коррупция : криминологический ежеквартальный альманах. 2003. Вып. 2. С. 141 ; Ее же. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы : дис. ... канд. юрид. наук. Владивосток, 2005. С. 12.

² Чекунов И. Г. Киберпреступность: понятие, классификация, современные вызовы и угрозы // Молодые ученые. 2012. № 3. С. 185 ; Его же. Криминологическое и уголовно-правовое обеспечение предупреждения киберпреступности : дис. ... канд. юрид. наук. М., 2013. С. 7.

³ Шарыпова Т. Н., Сидоренко А. А. Киберпреступность в XXI веке // Аллея науки. 2019. Т. 2, № 1(28). С. 975.

ных носителей информации или средств связи, при совершении киберпреступлений).

6. По А. Л. Осипенко, «киберпреступность» определяется особой подготовленностью преступников, повышенной скрытностью, трансграничным, дистанционным характером и многообразием способов совершения преступлений¹ (это наиболее полный перечень обстоятельств и признаков, свойственных большинству преступлений, совершаемых в глобальных компьютерных сетях, но необходимо помнить, что все они применимы к характеристике преступлений, совершаемых с использованием информационно-телекоммуникационных технологий).

Основным тезисом нашего исследования является идея о том, что преступления в сфере компьютерной информации – это лишь часть преступлений, входящих в структуру киберпреступности².

Необходимо выделить работы казахстанских исследователей, которые занимались проблемами киберпреступности: Б. Х. Толеубековой «Проблемы совершенствования борьбы с преступлениями, совершаемыми с использованием компьютерной техники» (1998)³, Т. Б. Сеитова «Международно-правовое сотрудничество государств в борьбе с компьютерной преступностью» (2002)⁴, А. К. Нурпеисовой «Уголовно-правовые и криминалистические аспекты компью-

¹ *Осипенко А. Л.* Сетевая компьютерная преступность: теория и практика борьбы : монография. Омск, 2009. С. 109–110.

² *Карабеков К. О.* Актуальные вопросы исследования киберпреступности в Российской Федерации и Республике Казахстан // Актуальные проблемы борьбы с преступлениями и иными правонарушениями : мат-лы двадцатой междунар. науч.-практ. конф. Ч. 2. Барнаул, 2022. С. 26.

³ *Толеубекова Б. Х.* Проблемы совершенствования борьбы с преступлениями, совершаемыми с использованием компьютерной техники : дис. ... д-ра юрид. наук. Алматы, 1998. 380 с.

⁴ *Сеитов Т. Б.* Международно-правовое сотрудничество государств в борьбе с компьютерной преступностью : дис. ... канд. юрид. наук. Алматы, 2002. 120 с.

терной преступности» (2010)¹, К. Аратулы «Уголовная политика в борьбе с компьютерной преступностью в условиях глобализации» (2013)².

Ученые Казахстана рассматривают киберпреступность как компьютерную преступность в уголовно-правовом, уголовно-процессуальном, криминалистическом аспектах (Б. Х. Толеубекова, Т. Б. Сеитов, А. К. Нурпеисова).

Отдельного внимания заслуживают научные труды К. Аратулы, который занимался исследованием компьютерной преступности в криминологическом аспекте. Согласно результатам его научных исследований к числу компьютерных преступлений можно отнести преступления в сфере компьютерной информации и преступления, совершаемые с использованием информационных технологий³. По его мнению, в зависимости от объекта и предмета посягательства все компьютерные преступления, предусмотренные как в отечественном, так и в зарубежном уголовном праве, можно разделить на две группы:

1. Преступления в сфере компьютерной информации. Предметом в таких преступлениях выступает компьютерная информация, как, например, в деяниях, предусмотренных ст. 227 УК РК; ст. ст. 272–274 УК РФ; ст. ст. 361–363 УК Украины; §1030(a) (1) Свода законов США «Несанкционированный доступ к информации с ограниченным доступом, касающейся национальной безопасности, международных отношений, атомной энергетики»; ст. 478.1 УК Австралии «Несанкционированный доступ или модификация охраняемой компьютерной информации или программы» и др.

2. Преступления, где компьютерная информация является орудием или средством совершения другого преступления. Эти составы преступлений указаны в других главах уголовных кодексов, например, в ст. 212 УК Республики Беларусь «Хищение путем использования компьютерной техники»; §1030(a) (7) Свода законов США «Вымогательство, угрозы причинения вреда с использованием ком-

¹ Нурпеисова А. К. Уголовно-правовые и криминалистические аспекты компьютерной преступности : автореф. дис. ... канд. юрид. наук. Караганда, 2010. 33 с.

² Аратулы К. Уголовная политика в борьбе с компьютерной преступностью в условиях глобализации (на казахском языке) : дис. ... д-ра философии (PhD). Алматы, 2013. 166 с.

³ Аратулы К. Преступления в сфере компьютерной информации в РК и зарубежных странах. URL: <https://articlekz.com/article/10037> (дата обращения: 14.09.2022).

пьютера»; ст. 206(1) (е) УК Канады «Использование компьютерных данных и технологий в целях извлечения прибыли путем создания финансовых пирамид» и др.

По Уголовному кодексу Российской Федерации ответственность за преступления этой группы должна наступать по иным статьям кодекса в соответствии с их родовым и непосредственным объектами. Однако такие деяния в необходимых случаях могут квалифицироваться по совокупности с преступлениями, предусмотренными ст. ст. 272–274 УК РФ.

По мнению казахстанских исследователей, на сегодняшний день в Казахстане наблюдаются все признаки институционализации киберпреступности, так как правовые нормы формируются в борьбе с киберпреступниками, создаются международные институты по кибербезопасности, развиваются новые сферы деятельности, ориентированные на противодействие киберпреступности, и др. (К. К. Сабиров, Ф. Р. Ахмеджанов). В Республике Казахстан также существует техническая и правовая база для создания системы безопасности киберпространства и сетей телекоммуникаций¹.

На наш взгляд, понятие киберпреступности в Республике Казахстан используется в широком смысле, а единого, полного и точного определения киберпреступности не дают ни законодатель, ни казахстанские исследователи.

Сегодня существует много способов совершения киберпреступлений, но не все из них актуальны на данный момент: часть устарела, другая требует от хакера большого опыта, а третьи просто не подходят для достижения цели преступника. В связи с этим злоумышленники очень серьезно выбирают способ совершения киберпреступления.

Под способом совершения преступления обычно понимают объективно и субъективно обусловленную систему поведения субъекта до, в момент и после совершения преступления, оставляющего различного рода характерные следы, позволяющие с помощью криминалистических приемов и средств получить представление о сути происшедшего, своеобразии противоправного поведения пре-

¹ Сабиров К. К., Ахмеджанов Ф. Р. Некоторые вопросы законодательного укрепления кибербезопасности в Республике Казахстан // Вопросы кибербезопасности. 2017. № 3(21). С. 56.

ступника, его отдельных личностных данных, что позволяет определить оптимальные методы решения задач в целях раскрытия преступления¹.

Согласно статистической отчетности ГИАЦ МВД России об уголовных преступлениях и по данным МВД РК об уголовных правонарушениях, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, указанная группа преступлений (уголовных правонарушений) совершается с использованием или применением расчетных (пластиковых) карт, компьютерной техники, программных средств, фиктивных электронных платежей, сети Интернет, средств мобильной связи.

Посредством исследования основных методов совершения киберпреступлений была проведена систематизация признаков понятия «киберпреступность», анализ которой не определяет единого мнения среди ученых в интерпретации термина «киберпреступность», что, соответственно, обусловливается различными трактовками киберпространства и способов использования компьютерных систем при совершении противоправных действий. Однако при наличии рассмотренных различий ученые ставят вопрос о соотношении общего международного законодательства и частного законодательства Российской Федерации по поводу перечня противоправных действий, которые отнесены к преступлениям, совершаемым в киберсфере.

По нашему мнению, понятие «киберпреступность» может применяться к преступлениям, которые совершаются с использованием любых средств информационно-коммуникационных технологий. Киберпреступность – это более широкое понятие, чем интернет-преступность, так как оно включает в себя возможность совершения преступлений с использованием любых информационных или телекоммуникационных сетей. Сеть Интернет – самая популярная сеть, но существуют и другие сети, которые могут быть использованы преступниками в качестве средства совершения преступления: ANts P2, Bitmessage, Freenet, Gnutella,

¹ Ушатиков А. И., Ковалев О. Г., Корнеева Г. К. Прикладная криминальная психология : учеб. пособие. Рязань, 2012. 596 с.

Manolito, MUTE, Nodezilla, OneSwarm, RShare, ZeroNet, TOR (The Onion Router), StealthNet, Hyperboria, JAP (Java Anonymous Proxy)¹.

Проблемы борьбы и предупреждения киберпреступлений начинаются с того, что не разработаны методологические основы изучения закономерностей данной группы преступности в информационном пространстве, где последнее следует понимать как «совокупность информационных ресурсов, созданных субъектами информационной сферы, средств взаимодействия таких субъектов, их информационных систем и необходимой информационной инфраструктуры»².

Изучив и оценив подходы к пониманию киберпреступности, изложенные в трудах ученых России и Казахстана, с точки зрения содержания ее признаков, следует выделить основные характеристики киберпреступности: 1) это преступность в информационном пространстве; 2) объектом преступления являются информационная безопасность, собственность, авторское право, общественная безопасность, нравственность; 3) она охватывает все преступные деяния, которые совершаются с использованием средств информационно-телекоммуникационных технологий; 4) ей присуща повышенная латентность, которая обеспечена спецификой сетевого информационного пространства (развитые механизмы анонимности, сложность инфраструктуры и т. п.)³; 5) носит дистанционный характер преступных действий в условиях отсутствия физического контакта преступника и потерпевшего, а также включает в себе возможность совершения преступления в автоматизированном режиме, т. е. в нескольких местах одновременно⁴; 6) обладает высоким потенциалом развития, способным наращивать неблагоприятные последствия, что приводит к дальнейшей невозможности предотвращения и пресечения преступлений данного вида традиционными средствами; 7) несоответствие темпа роста преступной деятельности в киберпространстве темпам законодатель-

¹ Анонимные сети. URL: <https://ru.wikipedia.org/wiki/> (дата обращения: 19.07.2022).

² *О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы* : Указ Президента Российской Федерации от 9 мая 2017 г. № 203 // Собрание законодательства Российской Федерации. 2017. № 20, ст. 2901.

³ Номоконов В. А. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. 2012. № 1. С. 46.

⁴ Пинкевич Т. В. Современные угрозы криминологической безопасности России // Философия права. 2021. № 3 (98). С. 92.

ного регулирования и реализации отдельных средств противодействия такой деятельности¹. Наиболее значимые из них положены нами в наше определение.

Учитывая вышеизложенные выводы, положения законодательных норм о киберпреступлениях и мнения исследователей о специфических признаках «киберпреступности», предлагаем под киберпреступностью в Российской Федерации и Республике Казахстан 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-коммуникационных технологий². При этом следует учитывать, что содержание киберпреступности в России и Казахстане фактически определяется совокупностью разнородных преступлений (уголовных правонарушений в Республике Казахстан), совершаемых с использованием компьютерной информации и информационно-телекоммуникационных технологий в целях удовлетворения потребностей преимущественно корыстной направленности.

§ 2. Состояние и тенденции киберпреступности

Состояние преступности в теории криминологии понимается по-разному: 1) по мнению Ю. М. Антоняна, «состояние преступности – это количество зарегистрированных преступлений в определенное время в той или иной стране (регионе, городе, районе и т. д.)»³; 2) на взгляд Н. А. Стручкова, «под состоянием преступности чаще всего понимается ее количественная характеристика: сколько совершено преступлений за какой-то период, в какой-то местности. Однако... для количественной характеристики преступности больше подходит другой термин – уровень, как числовое значение того или иного статистического показателя. Признак состояния преступности носит комплексный характер: оно определяется

¹ *Карабеков К. О.* Понятие киберпреступности в Российской Федерации и Республике Казахстан // Известия Юго-Западного государственного университета. Серия «История и право». 2022. Т. 12, № 5. С. 98.

² Там же. С. 99.

³ *Антонян Ю. М.* Криминология : избранные лекции. М., 2004. С. 76.

уровнем, структурой, динамикой и коэффициентом преступности»¹; 3) с точки зрения М. П. Клеймёнова, В. Д. Малкова, Г. А. Аванесова, состояние преступности – это интегральный показатель ее количественных и качественных характеристик² (данный подход считается классическим).

При этом следует помнить, что криминологи рассматривают саму преступность как статистическую совокупность преступлений³. Состояние преступности используется как интегральный показатель качественных и количественных характеристик в официальных статистических отчетах правоохранительных органов и имеет следующие цели:

1) определение уровня преступности. Целью может быть оценка количества и типов преступлений, которые происходят в какой-либо области или стране, что помогает понять, насколько общество защищено от преступности, и выделять приоритеты в области правоохранительной деятельности;

2) идентификация проблемных областей. Изучение состояния преступности способно выявить географические области или социальные группы, где преступность наиболее распространена, что позволяет сконцентрировать ресурсы правоохранительных органов, чтобы эффективно бороться с ней;

3) оценка эффективности правоохранительной системы. Изучение состояния преступности позволяет оценить эффективность правоохранительных органов и систем, включая анализ доли раскрытых преступлений, времени разбирательства дел, распределения ресурсов и мер предупреждения преступности, что помогает выявить проблемы в системе и предложить реформы для повышения ее эффективности;

4) поддержка разработки политики безопасности. Изучение состояния преступности может служить важным инструментом для разработки политики безопасности на уровне государства или регионов, на основе данных и анализа кото-

¹ Стручков Н. А. Преступность как социальное явление. Л., 1979. С. 14–15.

² Клеймёнов М. П. Криминология : учебник. М., 2018. С. 45 ; *Криминология : учебник* / под ред. В. Д. Малкова. М., 2004. С. 51 ; *Криминология : учебник* / Г. А. Аванесов, С. М. Иншаков, Е. А. Антонян [и др.] ; под ред. Г. А. Аванесова. 7-е изд., перераб. и доп. М., 2020. С. 67.

³ Вицин С. Е. Системный подход и преступность : учеб. пособие. М., 1980. С. 24.

рых выстраивается состояние преступности, в связи с чем возможно определить приоритеты по предупреждению и борьбе с преступностью, а также оценить эффективность принятых мер.

Киберпреступление отличается от традиционного преступления тем, что оно «не признает физические или географические границы», может совершаться с меньшими усилиями, большей легкостью, с большей скоростью, чем традиционное преступление¹ (хотя это зависит от вида киберпреступления и вида традиционного преступления, с которым оно сравнивается). Это связано с тем, что киберпреступность развивается стремительными темпами во многих странах, особенно тех, которые активно используют достижения цифровизации.

Обращаясь к опыту цифровизации стран Содружества Независимых Государств, следует обратить внимание на достижения Республики Казахстан и Российской Федерации в указанной сфере. Так, в 2024 г. по уровню цифровизации и диджитализации (индекс (E-Government Development Index, EGDI)) Казахстан занял 24-е, Россия – 43-е место среди 193 стран, входящих в мониторинг ООН. К сведению, Армения – 48-е, Беларусь – 58-е место, Узбекистан – 63-е, Молдова – 72-е, Азербайджан – 74-е, Кыргызстан – 81-е, Таджикистан – 129-е, Туркменистан – 137-е место². В то время, как в 2022 году Казахстан занимал 28-е место, Россия – 42-е, Беларусь – 58-е место, Армения – 64-е, Узбекистан – 69-е, Молдова – 72-е, Кыргызстан – 81-е, Азербайджан – 83-е, Таджикистан – 129-е, Туркменистан – 137-е место³.

Из всех стран Содружества Независимых Государств наиболее значительный рост киберпреступлений отмечается в Российской Федерации и Республике Казахстан. В России доля киберпреступлений в общей структуре зарегистрированных преступлений составляла 4,2% в 2016 г., к 2023 г. она увеличилась в во-

¹ *Киберпреступность*. Модуль 1. Введение в киберпреступность. Вена, 2019. С. 9.

² *Казахстан по уровню цифровизации опередил все страны СНГ*. URL: <https://liter.kz/kazakhstan-odna-iz-luchshikh-stran-v-mire-po-urovniu-tsifrovizatsii/> (дата обращения: 09.03.2025).

³ *Казахстан по уровню цифровизации опередил все страны СНГ*. URL: <https://liter.kz/kazakhstan-odna-iz-luchshikh-stran-v-mire-po-urovniu-tsifrovizatsii/> (дата обращения: 09.02.2024).

семь раз и составила 34,8%¹. Более негативная динамика киберпреступности наблюдалась в Казахстане. Несмотря на снижение регистрации общей преступности с 2016 г. по 2023 г. на 61,22%, доля киберпреступлений в общей структуре зарегистрированных преступлений с 2016 г. увеличилась в 73 раза. Так, в 2016 г. она составляла 0,24%, в 2023 г. – 17,5%². В 2024 г. данные тенденции продолжились.

Киберпреступность набирает обороты значительно быстрее, чем все другие виды преступности. В настоящее время киберпреступления представляют быстрый рост сегмента преступности, что связано с увеличением численности пользователей гаджетов, подключенных к глобальной сети. Любые информационные и технические новации значительно расширяют сферу криминальных деяний в информационно-телекоммуникационной среде и создают условия для повышения эффективности хакерских атак³.

В январе–декабре 2024 г. в Российской Федерации зарегистрировано 765,4 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, что на 13,1% больше, чем за аналогичный период прошлого года. В общем числе зарегистрированных преступлений их удельный вес увеличился с 34,8% в январе–декабре 2023 г. до 40,0%⁴.

За вышеуказанный период в Республике Казахстан было зарегистрировано 25 074 уголовные правонарушения с использованием информационной системы и в сфере информатизации и связи, что на 2,32% больше, чем за аналогичный период 2023 г.⁵

¹ *Состояние преступности в России за январь–декабрь 2023 г.* URL: <http://crimestat.ru/> (дата обращения: 09.02.2024).

² *Статистические данные – сведения об уголовных правонарушениях за 2016–2023 годы.* URL: <https://qamqor.gov.kz> (дата обращения: 09.02.2024).

³ Гундериц Г. А. Состояние киберпреступности // Научный вестник Крыма. 2018. № 4. С. 15.

⁴ *Состояние преступности в России за январь–декабрь 2024 г.* URL: <https://crimestat.ru/> (дата обращения: 09.02.2025).

⁵ *Статистические данные – сведения об уголовных правонарушениях за 2024 г.* URL: <https://qamqor.gov.kz> (дата обращения: 09.02.2025).

При анализе киберпреступности следует учитывать, что в Казахстане она образуется не только преступлениями, но и уголовными проступками¹, поскольку с 3 июля 2014 г. с принятием Уголовного кодекса Республики Казахстан впервые введена новая классификация уголовных правонарушений².

При изучении киберпреступности в России и Казахстане, наряду с абсолютными данными, использовались и относительные, такие как коэффициенты, удельный вес.

Сравнительный анализ распространенности киберпреступности в России и Казахстане показывает следующее (табл. 1):

- киберпреступлений (уголовных правонарушений в Казахстане) на 100 тыс. всего населения в Российской Федерации совершается в 3,6 раза больше, чем в Республике Казахстан;
- киберпреступлений (уголовных правонарушений в Казахстане) на 100 тыс. лиц в возрасте 14 лет и старше в Российской Федерации приходится в 3 раза больше, чем в Республике Казахстан;
- удельный вес киберпреступлений (уголовных правонарушений в Казахстане) в общем числе зарегистрированных преступлений в Российской Федерации в 2 раза больше, чем в Республике Казахстан;
- криминальная активность населения по киберпреступлениям (уголовных правонарушений в Казахстане) на 100 тыс. лиц в возрасте 14 лет и старше в Российской Федерации в 3 раза выше, чем в Республике Казахстан.

¹ Уголовным проступком признается совершенное виновно деяние (действие либо бездействие), не представляющее большой общественной опасности, причинившее незначительный вред либо создавшее угрозу причинения вреда личности, организации, обществу или государству, за совершение которого предусмотрено наказание в виде штрафа, исправительных работ, привлечения к общественным работам, ареста, выдворения за пределы Республики Казахстан иностранца или лица без гражданства (п. 3 ст. 10 УК РК).

² Уголовные проступки в системе правонарушений Республики Казахстан: теоретические, правовые и организационные аспекты : монография / [коллектив авторов]. Косшы, 2020. 327 с.

Таблица 1 – Уровень, интенсивность и удельный вес киберпреступлений в Российской Федерации и Республике Казахстан в 2024 г.

Зарегистрированные киберпреступления		Россия	Казахстан
Абсолютное число		765 365	25 074
K_{Φ} на 100 тыс. всего населения		523	131
K_{Φ} на 100 тыс. лиц в возрасте 14 лет и старше		633	184
Удельный вес в общем числе зарегистрированных преступлений, %		40,0	18,9
Выявлено лиц, совершивших преступления			
Абсолютное число		666 260	60 559
$K_{\text{л}}$ на 100 тыс. лиц в возрасте 14 лет и старше		551	445
Выявлено лиц, совершивших киберпреступления			
Абсолютное число		98 088	2960
$K_{\text{л}}$ на 100 тыс. лиц в возрасте 14 лет и старше		81	22
Удельный вес в общем числе выявленных лиц, совершивших киберпреступления, %		15	5

Примечания: K_{Φ} – коэффициент преступности; $K_{\text{л}}$ – коэффициент криминальной активности населения.

По итогам 2024 г. в России 48,2% зарегистрированных киберпреступлений относятся к категориям тяжких и особо тяжких (369,3 тыс.; +7,8%), четыре преступления из пяти (84,8%) совершаются с использованием сети Интернет (649,1 тыс.; +23,2%), почти половина (45,2%) – средств мобильной связи (346,0 тыс.; +14,3%).

По данным ГИАЦ МВД России, почти две трети таких преступлений (63,5%) совершается путем кражи или мошенничества, а именно – 486,3 тыс. (+2,3%); почти каждое восьмое (12,4%), – в целях незаконного производства, сбыта или пересылки наркотических средств, а именно 94,6 тыс. (+16,1%)¹.

К сожалению, Министерством внутренних дел Республики Казахстан (далее – МВД РК) и Комитетом по правовой статистике и специальным учетам Генеральной прокуратуры Республики Казахстан соответствующая информационно-аналитическая работа, которая ведется в этом направлении, не представляется в открытом доступе, поэтому нет возможности оценить киберпреступность по вышеуказанным показателям.

¹ Состояние преступности в России за январь–декабрь 2024 г. URL: <http://crimestat.ru/> (дата обращения: 09.02.2025).

Одним из компонентов организации противодействия преступности является его информационно-аналитическое обеспечение. Систематическое накопление достоверной, характеризующей оперативную обстановку информации, ее своевременный и качественный анализ, принятие на этой основе управленческих решений выступает главным условием научно обоснованной организации борьбы с преступностью¹.

Учитывая положительный опыт ГИАЦ МВД России и переход на сервисную модель полиции² в Казахстане, в целях обеспечения прозрачности работы перед населением предлагаем на официальном сайте МВД РК представлять ежемесячный аналитический обзор о состоянии киберпреступности в Казахстане. Это обосновано тем, что структура преступности отражает различные виды преступлений и их распределение по категориям (например, по тяжести, по сферам жизнедеятельности, по возрасту преступников и т. д.) позволяет оценить общую картину преступности в определенном регионе или стране, а также выявить тенденции и изменения в динамике преступности³.

Структура киберпреступности в России и Казахстане отличается. В России наиболее распространены такие виды киберпреступлений, как мошенничество, кража, незаконное производство, сбыт или пересылка наркотических средств, психотропных веществ, незаконный сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества. В Казахстане наиболее распространенным видом киберпреступлений является интернет-мошенничество.

¹ Иванов Н. Н. Интенсификация информационного обеспечения управления: проблемы и пути решения // Интенсификация информационного обеспечения управления в органах внутренних дел : тр. Академии МВД России. М., 1992. С. 3.

² Сервисная полиция – это подход к полицейской деятельности, согласно которому стратегия службы направлена на оказание качественных услуг населению и решение проблем безопасности в партнерстве с обществом. Основными направлениями в развитии сервисной модели являются профилактика преступлений и правонарушений, шаговая доступность, нацеленная на максимальное облегчение гражданам доступа к полиции (*Сервисная модель: Новые механизмы и методы работы столичной полиции*. URL: <https://tengrinews.kz/news/servisnaya-model-povuyie-mehanizmyi-metodyi-raboty-456216/> (дата обращения: 03.05.2024)).

³ Клишков В. Б., Пасынков В. В., Стебенева Е. В. Преступность и ее основные характеристики на современном этапе // Вестник Санкт-Петербургского университета МВД России. 2015. № 4(68). С. 158.

ГИАЦ МВД России объединяет преступления в сфере компьютерной информации и совершаемые с использованием информационно-телекоммуникационных технологий в одну группу¹. Таким образом, структура киберпреступности в России образована двумя видами преступлений: «преступления в сфере компьютерной информации» и «преступления, совершаемые с использованием информационно-телекоммуникационных технологий». Первая группа – это преступления в сфере компьютерной информации (ст. ст. 272–274² Уголовного кодекса Российской Федерации (далее – УК РФ))². Вторая группа киберпреступлений – это все преступления, совершающиеся с помощью информационно-телекоммуникационных технологий (п. «г» ч. 3 ст. 158, ст. ст. 159³, 159⁶, 171², ч. 2 ст. 205², п. «б» ч. 2 ст. 228¹, п. «б» ч. 3 ст. 242, п. «г» ч. 2 ст. 242¹, п. «г» ч. 2 ст. 242², ч. 2 ст. 280 УК РФ).

По данным Центра по борьбе с киберпреступностью Департамента криминальной полиции МВД РК³, структуру киберпреступности Казахстана образуют уголовные правонарушения, совершаемые в сфере информатизации и связи, и с использованием информационных технологий⁴.

Уголовные правонарушения в сфере информатизации и связи, которые предусмотрены в главе 7 Уголовного кодекса Республики Казахстан (далее – УК РК), представлены в виде девяти статей (ст. ст. 205–213)⁵. В 2024 г. доля данных уголовных правонарушений в структуре киберпреступности в Казахстане составила всего 0,28%, в 2023 г. – 0,33 % (табл. 2).

¹ О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности : указание Генеральной прокуратуры Российской Федерации и МВД России от 30 июня 2022 г. № 361/11/1. Доступ из справ.-правовой системы «КонсультантПлюс».

² Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

³ Официальный сайт Министерства внутренних дел Республики Казахстан (МВД РК). URL: <https://www.gov.kz/memleket/entities/qriim> (дата обращения: 09.02.2024).

⁴ Статистические данные – сведения об уголовных правонарушениях за 2023 год. URL: <https://qamqor.gov.kz> (дата обращения: 09.02.2024).

⁵ Уголовный кодекс Республики Казахстан от 3 июля 2014 г. № 226-V ЗПК. URL: <https://adilet.zan.kz/rus/docs/> (дата обращения: 09.02.2024).

Таблица 2 – Сравнение структуры киберпреступности в России и Казахстане

Преступления (уголовные правонарушения)	Россия, %	Казахстан, %
Мошенничества (ст. ст. 159, 159 ³ , 159 ⁶ УК РФ; п. 4 ч. 2 ст. 190 УК РК)	49,69	89,97
Кража (ст. 158 УК РФ; п. 4 ч. 2 ст. 188 УК РК)	13,84	4,49
Преступления в сфере компьютерной информации (глава 28 УК РФ; глава 7 УК РК)	13,82	0,28
Незаконные производство, сбыт или пересылка наркотических средств, психотропных веществ, а также незаконные сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества (ст. 228 ¹ УК РФ; п. 5 ч. 3 ст. 297, п. 3 ч. 2 ст. 299, п. 4 ч. 2 ст. 299-1, п. 4 ч. 3 ст. 301 УК РК)	12,37	4,81
Изготовление порнографических материалов (ст. ст. 242, 242 ¹ , 242 ² УК РФ; ст. ст. 311, 312 УК РК)	0,46	0,1
Публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма (ст. 205 ² УК РФ; ч. 2 ст. 256 УК РК)	0,12	0,03
Публичные призывы к осуществлению экстремистской деятельности (ст. 280 УК РФ) Разжигание социальной, национальной, родовой, расовой, сословной или религиозной розни ч. 1 ст. 174 УК РК)	0,06	0,26
Незаконные организация и проведение азартных игр (ст. 171 ² УК РФ)	0,05	–
Незаконные изготовление, производство, приобретение, сбыт или использование специальных технических средств негласного получения информации (ч. 1 ст. 399 УК РК)	–	0,06
Иные киберпреступления	9,59	–

Вторая группа киберпреступлений в Республике Казахстан – это все уголовные правонарушения, совершаемые с помощью информационных технологий. УК РК включает 30 составов таких уголовных правонарушений, но, по данным МВД РК, актуальными из них являются те, которые указаны в п. 4 ч. 2 ст. 188, п. 4 ч. 2 ст. 190, п. 5 ч. 3 ст. 297, п. 3 ч. 2 ст. 299, п. 4 ч. 2 ст. 299-1, п. 4 ч. 3 ст. 301, ст. ст. 311, 312, ч. 1 ст. 399 кодекса.

Преступность в информационно-телекоммуникационном пространстве постоянно изменяется, поэтому существует необходимость учитывать ее состояние,

уровень и структуру на конкретной территории и за определенный период времени, т. е. наблюдать ее в динамике¹.

Анализ статистических данных показывает, что в Российской Федерации и Республике Казахстан, несмотря на колебания общего количества зарегистрированных преступлений, число зарегистрированных киберпреступлений неуклонно растет (табл. 3).

Таблица 3 – **Количество зарегистрированных киберпреступлений в 2016–2024 гг. в России² и Казахстане³**

Год	Показатель							
	Всего зарегистрированных преступлений в РФ	Темп прироста, %	Всего зарегистрированных киберпреступлений в РФ	Темп прироста, %	Всего зарегистрированных уголовных правонарушений в РК	Темп прироста, %	Всего зарегистрированных киберуголовных правонарушений в РК	Темп прироста, %
2016	2 160 063	–	90 722	–	361 689	–	902	–
2017	2 058 476	-4,94	142 034	56,56	316 418	-12,52	2869	218
2018	1 991 532	-3,36	175 254	23,39	292 286	-7,63	5058	76,3
2019	2 024 337	1,65	294 402	67,99	243 462	-16,70	8522	68,5
2020	2 044 221	0,98	510 447	73,38	162 783	-33,14	14 109	65,5
2021	2 004 404	-1,95	517 722	1,43	157 884	-3,01	21 479	52,2
2022	1 966 841	-1,84	522 065	0,8	151 241	-4,21	20 531	-4,5
2023	1 947 161	-1,0	676 951	29,66	140 272	-7,25	24 506	19,36
2024	1 911 258	-1,8	765 365	13,1	132 778	-5,34	25 074	2,32

Согласно указанным данным, в России с 2016 г. по 2024 г. наблюдалось колебание общего числа зарегистрированных преступлений. За последние два года произошло снижение количества зарегистрированных преступлений, и к 2024 г. по сравнению с 2016 г. оно сократилось на 248 805 преступлений. Тем не менее число киберпреступлений неуклонно растет. В 2024 г. было зарегистрировано на 674 643 киберпреступления больше, чем в 2016 г. Количество рассматриваемых преступле-

¹ Омигов В. И. Некоторые формы и содержание прогноза развития преступности в России // Российский следователь. 2016. № 14. С. 35.

² Состояние преступности в России за январь–декабрь 2024 г. URL: <http://crimestat.ru/> (дата обращения: 09.02.2025).

³ Статистические данные – сведения об уголовных правонарушениях за 2016–2024 годы. URL: <https://qamqor.gov.kz> (дата обращения: 09.02.2025).

ний увеличилось на 844%. Изменение удельного веса от общего числа преступлений также указывает на их значительный рост (рис. 1).

Высокие темпы прироста киберпреступлений в Казахстане наблюдаются с 2017 г. (218%) по 2021 г. (52,2%). В 2016 г. было зарегистрировано 902 факта уголовных правонарушений с использованием информационных технологий и в сфере информатизации и связи; 2017 г. – 2869; 2018 г. – 5058; 2019 г. – 8522; 2020 г. – 14 109; 2021 г. – 21 479; 2022 г. – 20 531; 2023 г. – 24 506; 2024 г. – 25 074¹ (рис. 1).

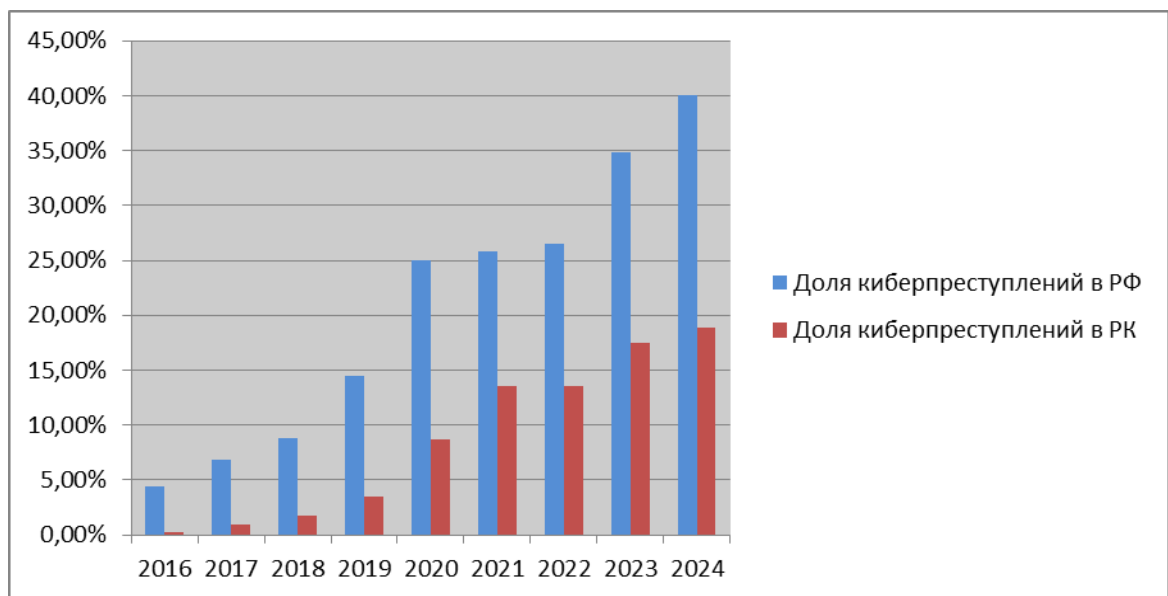


Рис. 1. Динамика удельного веса киберпреступлений в период с 2016 г. по 2024 г. в Российской Федерации² и Республике Казахстан³

Очевидно, что преступный мир неуклонно мигрирует в киберпространство, где ежегодно совершается все больше преступлений. Прогнозируется, что удельный вес киберпреступлений в России продолжит увеличиваться и в 2030 г. может превысить показатель 66% от общего числа зарегистрированных преступлений,

¹ Интернет-портал правовой статистики Генеральной прокуратуры Республики Казахстан. URL: <https://qamqor.gov.kz/portal/> (дата обращения: 09.02.2025) ; Современное состояние и тенденции развития киберпреступности на пространстве Содружества Независимых Государств : аналитический обзор с предложениями / Н. Н. Дьяченко, О. А. Надейкина, Д. В. Кирган, И. А. Грозан, В. А. Казакова, О. И. Новосельцев, О. В. Демковец. М., 2023. С. 45.

² Состояние преступности в России за январь–декабрь 2024 г. URL: <http://crimestat.ru/> (дата обращения: 09.02.2025).

³ Интернет-портал правовой статистики Генеральной прокуратуры Республики Казахстан. URL: <https://qamqor.gov.kz/portal/> (дата обращения: 09.02.2025).

а в Казахстане может составить более 44% всех зарегистрированных уголовных правонарушений (рис. 2).

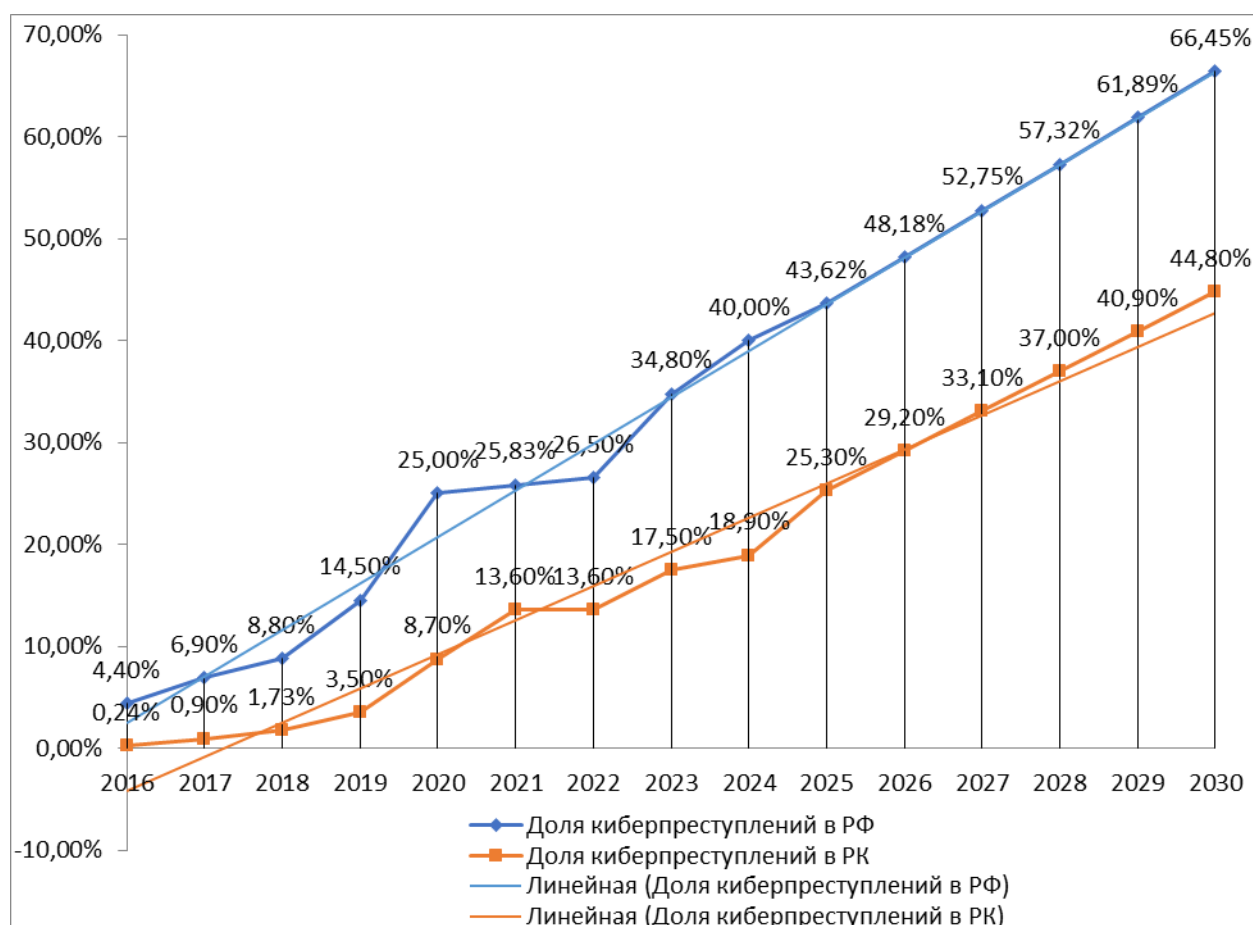


Рис. 2. Прогноз развития киберпреступности до 2030 г. в Российской Федерации¹ и Республике Казахстан²

Согласно статистической отчетности ГИАЦ МВД России о преступлениях и по данным МВД РК об уголовных правонарушениях, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, данная группа преступлений (уголовных правонарушений) совершается с использованием или применением расчетных (пластиковых) карт, компьютерной техники, программных средств, фиктивных электронных платежей, сети Интернет, средств мобильной связи.

¹ Состояние преступности в России за январь–декабрь 2024 г. URL: <http://crimestat.ru/> (дата обращения: 09.02.2025).

² Интернет-портал правовой статистики Генеральной прокуратуры Республики Казахстан. URL: <https://qamqor.gov.kz/portal/> (дата обращения: 09.02.2025).

По данным ГИАЦ МВД России, в 2024 г. с использованием или применением сети Интернет было совершено 649,1 тыс. (84,8%) киберпреступлений, средств мобильной связи – 346,0 тыс. (45,2%), расчетных (пластиковых) карт – 115 469 (15,09%), компьютерной техники – 42 347 (5,53%), программных средств – 13461 (1,76%), фиктивных электронных платежей – 615 (0,08%)¹.

В Республике Казахстан 89,97% уголовных правонарушений с использованием информационных технологий составляет мошенничество (п. 4 ч. 2 ст. 19 УК РК). Согласно информации МВД РК, в 2024 г. зарегистрировано 22 870 интернет-мошенничеств. Это больше показателя 2023 г., составлявшего 21 777 преступлений (темп прироста 5,02%). В результате действий мошенников в 2024 г. гражданам причинен ущерб на сумму более 45,5 млрд тенге (7,2 млрд рублей). Самым распространенным способом остается онлайн-торговля. Таким способом в 2024 г. совершено 7200 (31,48%) интернет-мошенничеств. Как правило, мошенники размещают объявления на сайтах и в социальных сетях, указывают заниженные цены за товар или услугу, просят предоплату либо полную оплату.

В рамках сравнительно-правового подхода был проведен анализ 316 приговоров, вынесенных судами РФ и РК по киберпреступлениям (прил. 5). С точки зрения совокупного материального ущерба установлено следующее: в РФ общий ущерб составил около 977 млн рублей при среднем размере ущерба на дело – 6,39 млн рублей; в РК – 2,58 млрд тенге, средний ущерб на дело – 15,8 млн тенге. Наибольший ущерб в обеих странах зафиксирован по делам, связанным с: интернет-мошенничеством (ст. 159 УК РФ / ст. 190 УК РК); киберпреступлениями в сфере компьютерной информации (ст. ст. 272–273 УК РФ / ст. ст. 205, 210 УК РК).

Анализ показывает, что, несмотря на наличие различий в структуре уголовного законодательства (в частности, отсутствие прямых аналогов ст. ст. 159³, 159⁶ УК РФ в УК РК), в этих государствах имеется сходство при

¹ *Состояние преступности в России за январь–декабрь 2016–2024 гг.* URL: <http://crimestat.ru/> (дата обращения: 09.02.2025).

подходе к оценке общественной опасности преступлений данной категории, а также к их квалификации и репрессивному реагированию. Следует отметить, что по ряду составов преступлений в РК наблюдаются более высокие показатели материального ущерба, что может быть обусловлено как особенностями судебной оценки, так и спецификой делового и финансового оборота.

Таким образом, правоприменительная практика по рассматриваемым категориям дел в РФ и РК демонстрирует как общее направление уголовной политики в части борьбы с киберпреступностью, так и отдельные особенности, имеющие значение для дальнейшей гармонизации и сближения уголовно-правовых подходов в рамках евразийского правового пространства.

Согласно данным МВД РК, большинство интернет-мошенничеств, связанных с оформлением на граждан кредитов и займов, а также хищением их банковских накоплений, совершаются «зарубежными преступниками». Они входят в состав транснациональных организованных преступных групп, работающих по принципу «Call-центров» с постоянной дислокацией в странах ближнего и дальнего зарубежья.

Наблюдая рост регистрации интернет-мошенничеств, можно говорить о недостаточности и малоэффективности проводимых мер по предупреждению и профилактике данных деяний, а также о доверчивости и правовой неграмотности граждан, бесконтрольном распространении мошеннических мобильных приложений, об открытой рекламе финансовых интернет-пирамид, малоэффективности существующих мер киберзащиты платежных интернет-платформ, нехватке специалистов по кибербезопасности и пр.¹

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

¹ Мухамеджанова А. Д. Особенности динамики киберпреступности в Республике Казахстан и ее влияние на вопросы ее предупреждения // Российско-азиатский правовой журнал. 2022. № 2. С. 52.

зарегистрированных преступлений составляла 40,0%¹, то в Казахстане она была значительно меньше – 18,9%².

Во-вторых, это отличие проявляется в темпах роста киберпреступности. В 2016 г. в России доля киберпреступлений в общей структуре зарегистрированных преступлений составляла 4,2%, а к 2024 г. она увеличилась в 9,5 раза и составила 40,0%³. 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%⁴.

Структура киберпреступности в России и Казахстане состоит из двух групп преступлений (уголовных правонарушений в Казахстане): киберпреступления в сфере компьютерной информации и киберпреступления, совершенные с использованием информационно-коммуникационных технологий.

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%), незаконное производство, сбыт или пересылка наркотических средств, психотропных веществ, а также незаконный сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества (12,37%).

В Республике Казахстан распространенным видом уголовных киберправонарушений в общей структуре общей преступности является мошенничество (89,97%).

Соответствующую оценку состояния преступности в России и Казахстане дают и сотрудники правоохранительных органов этих стран. Так, по результатам

¹ *Состояние* преступности в России за январь–декабрь 2023 г. URL: <http://crimestat.ru/> (дата обращения: 09.02.2024).

² *Статистические данные* – сведения об уголовных правонарушениях за 2016–2023 годы. URL: <https://qamqor.gov.kz> (дата обращения: 09.02.2024).

³ *Состояние* преступности в России за январь–декабрь 2023 г. URL: <https://crimestat.ru/> (дата обращения: 09.02.2024).

⁴ *Статистические данные* – сведения об уголовных правонарушениях за 2016–2023 годы. URL: <https://qamqor.gov.kz> (дата обращения: 09.02.2024).

опроса 50% сотрудников правоохранительных органов Российской Федерации и 49,79% сотрудников правоохранительных органов Республики Казахстан оценивают уровень киберпреступности как высокий и до 20% опрошенных в каждой стране – как сверхвысокий. При этом 59,7% в России и 76,95% 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.

Результаты анализа позволяют сформулировать вывод о том, что киберпреступность в России и Казахстане носит корыстный характер.

Первоначальная гипотеза о том, что в стране, где более высокий уровень цифровизации, должен быть более высокий уровень киберпреступности, не подтвердилась. Несмотря на высокий уровень цифровизации в Республике Казахстан, данные свидетельствуют о более низком уровне киберпреступности в данном государстве по сравнению с Россией. Во многом это обусловлено активной работой по предотвращению киберпреступлений.

Учитывая положительный опыт ГИАЦ МВД России и переход на сервисную модель полиции в Казахстане, в целях обеспечения прозрачности работы перед населением предлагаем на официальном сайте МВД РК размещать ежемесячный аналитический обзор о состоянии киберпреступности в стране.

Значительную опасность начинает представлять мошенничество с использованием искусственного интеллекта¹. К 2023 г. уже существовало несколько способов использования искусственного интеллекта (далее – ИИ) для обмана или манипуляции людьми²: 1) фейковые новости и информация (создание и распространение фейковых новостей, текстов, изображений и видео с использованием ИИ для манипуляций мнением общественности); 2) социальные боты и манипуляция в социальных сетях: использование ИИ для создания автоматических ботов, кото-

¹ *Карабеков К. О.* Актуальность использования возможностей нейросетей в предупреждении преступности // Преемственность и новации в юридической науке : мат-лы междунар. науч. конф. адъюнктов, аспирантов и соискателей. 2023. Вып. 19. С. 50.

² *Топ-5 мошеннических схем с использованием искусственного интеллекта в 2023 году!* URL: <https://vc.ru/u/1902918-komalenkov-kirill-lirik/> (дата обращения: 28.11.2023).

рые «лайкают», комментируют и распространяют определенные сообщения для влияния на общественное мнение; 3) фишинг и мошеннические веб-сайты (использование ИИ для создания поддельных электронных писем (генерации любых писем) и веб-сайтов (парсинг и считывание любых веб-файлов, даже закрытых от индексации, и сразу генерация любых уникальных материалов взамен), чтобы обмануть пользователей и получить доступ к их личным данным и финансовым ресурсам); 4) мошенничество с голосом (ИИ может имитировать человеческий голос и совершать голосовые мошенничества, такие как звонки от фальшивых служб поддержки или обман на телефоне¹); 5) манипуляция рекомендациями и персональными данными (платформы и приложения могут использовать ИИ для манипуляции рекомендациями товаров, услуг и контента, основанными на персональных данных пользователей, с целью максимизировать прибыль)².

По мнению эксперта по направлению информационной безопасности Центра цифровой экспертизы Роскачества С. Кузьменко, «благодаря имеющимся технологиям, хакерам достаточно всего лишь 20-секундного фрагмента с разговором, взятым из социальной сети, для создания клона голоса любого человека. Идентичность поражает настолько, что даже мать не сможет отличить голос своего ребенка от робота»³.

Подводя итог изложенному, следует отметить, что основные криминологические показатели киберпреступности свидетельствуют о том, что, несмотря на более низкий уровень цифровизации, киберпреступлений в Российской Федерации совершается значительно больше, чем в Республике Казахстан, как в абсолютных, так и в относительных показателях. Например, в расчете на единицу населения в Российской Федерации киберпреступлений совершается в 3 раза больше, чем соответствующих уголовных правонарушений в Республике Казах-

¹ *Оссама К. Е.* Предупреждение киберпреступлений в США и России: криминологическая характеристика личности киберпреступника в США // Евразийский юридический журнал. 2022. № 2. С. 325.

² *Бегишев И. Р., Шутова А. А.* Регулирование технологий искусственного интеллекта: столкновение этики и закона // Лоббирование в законодательстве. 2025. Т. 4, № 1. С. 27.

³ *Мошенники* используют нейросети для копирования голоса и образа жертвы. URL: <https://news.rambler.ru/tech/> (дата обращения: 28.11.2023).

стан. При этом доля киберпреступлений в общей структуре зарегистрированных преступлений в России в 2 раза больше, чем в Казахстане. В то же время в Казахстане отмечаются значительно более высокие темпы роста киберпреступности, чем в Российской Федерации. За последние 8 лет они в три раза превышали темпы роста киберпреступности в России.

Важной характеристикой структуры киберпреступности как в России, так и в Казахстане является то, что в данных странах подавляющее количество киберпреступлений совершаются с использованием информационно-телекоммуникационных технологий. Среди них в России около 64% (АППГ – 63,8%) занимают киберпреступления против собственности, среди которых больше всего распространены кибермошенничество и киберкража (50 и 14% соответственно). В Республике Казахстан киберправонарушения против собственности составляют еще большую долю – более 94% (АППГ – 94,46%), но среди них наибольшую распространенность имеет только кибермошенничество (90 и 4% соответственно).

Поскольку указанные выше признаки носят устойчивый характер, определяют особенности состояния и структуры общей преступности в Российской Федерации и Республике Казахстан, наблюдаются в большинстве регионов, их можно рассматривать как один из основных видов национальной преступности¹.

При этом предполагаемые направления развития киберпреступлений, совершаемых с использованием ИИ, связаны с облегчением доступа в информационно-телекоммуникационную сферу лиц, имеющих минимальные технические знания, позволяющие даже неподготовленным преступникам эффективно осуществлять кибератаки и организовывать сложные схемы мошенничества. Прогнозируются расширение спектра преступлений, совершаемых с использованием ИТ-технологий, и увеличение масштабов кибератак, разработка новых сценариев киберпреступлений, связанных с преодолением языковых барьеров, усилением ме-

¹ *Карабеков К. О.* Состояние и тенденции киберпреступности в Российской Федерации и Республике Казахстан // Научный вестник Омской академии МВД России. 2023. № 3(93). С. 111.

тодов манипулирования сознанием, изменением контента для усложнения идентификации преступника.

§ 3. Особенности лиц, совершающих киберпреступления

Личность киберпреступника — это совокупность социально-демографических, нравственно-психологических и уголовно-правовых свойств человека, определяющих преступное поведение личности, выражающееся в совершении преступлений в киберпространстве.

Большое количество научных исследований, посвященных проблемам киберпреступности, криминологической характеристике личности киберпреступника, свидетельствует об актуальности данной темы.

На современном этапе развития цифрового общества существует необходимость провести комплексное исследование элементов, составляющих криминологическую характеристику киберпреступника: выяснить взаимосвязь особенностей личности киберпреступника с динамикой роста киберпреступлений, общественной опасности таких преступлений, размеров причиняемого материального ущерба и морального вреда¹.

Остаются неисследованными вопросы влияния информационных технологий на преступность в целом и личность преступника в частности, современную виктимность, а также на особенности предупреждения преступлений, совершаемых с использованием информационных технологий².

Для организации борьбы с киберпреступностью в Российской Федерации и Республики Казахстан большое значение имеет информация о лице, совершившем киберпреступление.

Киберпреступность обладает уникальными характеристиками, которые заключаются в использовании компьютерной информации и информационно-

¹ Евдокимов К. Н. Противодействие компьютерной преступности: теория, законодательство, практика : дис. ... д-ра юрид. наук. М., 2021. С. 101.

² Талан М. В., Шавалеев Б. Э. Криминологический анализ личности мошенника в сфере неправомерного использования электронных средств платежа // Вестник Санкт-Петербургского университета. Право. 2023. № 1. С. 110.

телекоммуникационных технологий для осуществления преступных действий. В России и Казахстане с помощью этих технологий совершаются разные преступления, включая мошенничество, кражи, торговлю наркотиками и психотропными веществами, продажу оружия, специальных средств, порнографических материалов, а также незаконную организацию и проведение азартных игр. Как показывает проведенный в предыдущем параграфе анализ, все эти деяния имеют общую корыстную мотивацию. Таким образом, киберпреступность в этих странах в значительной мере связана с корыстными мотивами¹.

В юридической литературе встречаются различные подходы к криминологической характеристике личности. Для полного понимания данной тематики необходимо первоначально определить общее криминологическое понятие современной личности преступника.

По мнению ученых-криминологов А. И. Долговой², Ю. М. Антоняна³, при употреблении понятия «личность преступника» следует иметь в виду социальные характеристики человека, совершившего преступление.

Данная позиция заключается в том, что человек не рождается личностью, а становится ею в ходе общения, следовательно, вне общества формирование личности невозможно (процесс социализации личности), т. е. человек не рождается преступником, а становится им в результате неблагоприятного морально-нравственного формирования его личности⁴.

На взгляд М. П. Клеймёнова, личность преступника – это совокупность социально значимых свойств, определяющих виновное совершение преступления, мера социальной патологии в человеке. Ученый обращает внимание, что личность

¹ *Карабеков К. О.* Некоторые вопросы борьбы с киберпреступностью в России // Проблемы и перспективы совершенствования законодательства и правоприменительной практики органов внутренних дел : мат-лы междунар. науч.-практ. конф., посвященной 30-летию казахстанской полиции. Караганда, 2022. С. 101.

² *Криминология* : учебник / под общ. ред. А. И. Долговой. 3-е изд., перераб. и доп. М., 2005. С. 330.

³ *Антонян Ю. М.* Криминология : избранные лекции. М., 2004. С. 74.

⁴ *Петровский А. В.* Преступное поведение как криминологическая категория и объект антикриминального предупредительного воздействия // Журнал правовых и экономических исследований. 2024. № 4. С. 179–185.

преступника – это социальный, а не биологический тип, и от личности не преступника она отличается не физиологическими, не биологическими, а нравственно-психологическими и социологическими признаками¹.

С. А. Григорян считает, что, исходя из общей криминологической трактовки «личности преступника», следует выделить понятие личности современного «киберпреступника». Личность современного киберпреступника есть совокупность нравственно-психологических, уголовно-правовых и социально-демографических качеств личности, выражающихся в преступном поведении индивида при совершении «киберпреступлений»². Основываясь на способах совершения киберпреступлений, С. А. Григорян предлагает выделить два типа киберпреступников: 1) обычные киберпреступники, совершающие противоправные действия отдельных видов преступной деятельности (мошеннические действия, наркоторговля посредством сети Интернет и т. д.); 2) преступники в среде компьютерной информации и технологий, которые могут вести противоправную деятельность только в киберпространстве (например, несанкционированный доступ к компьютерной информации и ресурсам и т. д.).

Дополнительно он выделяет типы личности киберпреступников, обусловленные мотивацией совершения преступности: 1) самоутверждающийся тип (лица, совершающие киберпреступления, должны считаться «кибергениями»); 2) неосторожный тип (для данного типа совершение преступления в киберпространстве неблагоприятно); 3) протестующий тип (для них совершение киберпреступлений выступает формой протеста, идеологической или политической борьбы); 4) корыстный тип (выражается в материальной и иной заинтересованности киберпреступника); 5) насильственный тип (киберпреступники данного типа без физического контакта совершают преступления против личности путем доведения жертвы до самоубийства в сети Интернет, с помощью угроз или иными методами психологического воздействия, также насильственным типом киберпреступника

¹ Клейменов М. П. Указ. соч. С. 89.

² Григорян С. А. Особенности личности современного «киберпреступника» // Наука и образование: хозяйство и экономика; предпринимательство; право и управление. 2022. № 8. С. 103.

может быть лицо, призывающее в сети Интернет к совершению преступлений террористического характера, последствиями которых является смерть граждан).

По мнению С. А. Григоряна, анализ личности киберпреступника играет немаловажную роль при расследовании и раскрытии преступлений, поскольку позволяет выявить детерминанты, способствующие росту киберпреступности, а также на их основании выработать меры профилактики и предупреждения киберпреступлений¹.

Согласно исследованию Ю. В. Белевитиной, анализ статистических данных и судебной практики позволяет сделать вывод, что среднестатистический киберпреступник – это лицо в возрасте от 16 до 40 лет, имеющее либо достаточно хорошие, либо профессиональные навыки работы с информационными технологиями и (или) вредоносными программами, проживающее в городской местности, не имеющее постоянного источника дохода, совершающее преступления из корыстных намерений. Составленный примерный портрет личности киберпреступника, совершившего преступление в сфере компьютерной информации, является достаточно условным и требует дальнейших углубленных криминологических исследований с учетом постепенного роста динамики данного вида преступности².

Исходя из структуры киберпреступности, можно выделить следующую классификацию личности киберпреступников: 1) кибермошенник; 2) кибервор; 3) киберпреступник в сфере компьютерной информации; 4) киберпреступник в сфере распространения наркотических и иных запрещенных законом веществ; 5) кибертеррорист; 6) киберэкстремист; 7) киберпреступник, распространяющий порнографические материалы.

Сравнение показывает, что количество выявленных лиц, совершивших киберпреступления, в общем объеме лиц, совершивших преступления в России, в три раза больше, чем в Казахстане. Так, в Российской Федерации в 2024 г. данный показатель

¹ Там же. С. 105–108.

² Белевитина Ю. В. Криминологический портрет личности киберпреступника в современной России // Инновационная наука. 2022. № 12–2. С. 64.

составил 98 088 человек (15% всех лиц, совершивших преступления)¹, в Республике Казахстан – 2960 (5% всех лиц, совершивших преступления)². В то время как в 2023 г. такое соотношение было два к одному (14 и 7% соответственно).

При этом нераскрываемость по киберпреступлениям превышает 70%, а значит, информация о преступниках правоохранным органам малоизвестна.

Таким образом, для составления портрета личности киберпреступника в орбиту исследования вошли данные о раскрытых преступлениях, где установлено лицо, совершившее деяние, и количественные показатели, касающиеся таких лиц.

Низкий уровень раскрываемости киберпреступлений во многом связан с уровнем подготовки и особенностями личности киберпреступника. Повышенная скрытность, трансграничный, дистанционный характер и многообразие способов совершения киберпреступлений дают преступникам возможность избежать наказания. Следует обратить внимание на то, что увеличивается общественная опасность этого явления в силу отсутствия на первоначальном этапе возникновения компьютерных сетей должного контроля со стороны государства за деятельностью в данной сфере. Это привело к формированию преступной активности в сети, в первую очередь, в таких видах преступлений, как похищение конфиденциальной информации, мошенничество в целях получения денежных средств, шпионаж, а также распространение объектов и услуг, входящих в перечень нелегальных (например, предоставление сведений относительно наркотической продукции, демонстрация детской порнографии и т. д.)³. Как показывает практика, данные действия, ранее реализуемые преступниками в офлайн-пространстве, в настоящее время успешно осуществляются ими при помощи интернет-технологий.

Рассмотрим значимые социально-демографические, нравственно-психологические, уголовно-правовые качества киберпреступников.

1. Социально-демографические качества киберпреступников.

¹ *Состояние преступности в России за январь–декабрь 2024 г.* URL: <http://crimestat.ru/> (дата обращения: 24.07.2025).

² *Статистические данные – сведения об уголовных правонарушениях за 2024 год.* URL: <https://qamqor.gov.kz> (дата обращения: 24.07.2025).

³ *Майстренко Г. А.* Киберпреступность в России: сущность, общественная опасность и методы борьбы // Вопросы российского и международного права. 2022. Т. 12, № 1А. С. 183–184.

Согласно отчету Судебного департамента при Верховном Суде Российской Федерации «О демографических признаках осужденных за мошенничество с использованием электронных средств платежа (ст. 159³ УК РФ) и в сфере компьютерной информации (ст. 159⁶ УК РФ)¹» выделяются следующие основные характеристики современного **интернет-мошенника**:

а) по проживанию на местности (постоянные жители данной местности – 91,28%; жители иной местности – 8,72%);

б) по образованию (имеют высшее профессиональное – 21,85%; среднее профессиональное – 41,03%; среднее общее – 28,81%; основное общее – 8,31%);

в) по возрасту (от 14 до 17 лет – 3,32%; от 18 до 24 лет – 29,81%; от 25 до 29 лет – 21,34%; от 30 до 49 лет – 41,78%; от 50 лет и старше – 3,75%);

г) по социальному статусу (рабочие – 13,75%; государственные и муниципальные служащие – 1,06%; служащие коммерческой или иной организации – 13,87%; лица, осуществляющие предпринимательскую деятельность или участвующие в предпринимательской деятельности, – 4,83%; учащиеся и студенты – 2,96%; нетрудоспособные (неработающие) – 6,08%; трудоспособные лица без постоянного источника дохода – 57,45%).

Представленные сведения свидетельствуют о том, что кибермошенником является лицо 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.

Анализ сводной статистики судов России за несколько лет подтверждает вывод о сохранении общих показателей. Так, сводная статистика судов Российской Федерации о демографических особенностях лиц, совершивших кражу с банковского счета, а равно в отношении электронных денежных средств, преду-

¹ *Отчет* о демографических признаках осужденных по всем составам преступлений УК РФ. Форма № 11.1 утверждена приказом Судебного департамента при Верховном Суде Российской Федерации от 11 апреля 2017 г. № 65. URL: http://www.cdep.ru/userimages/sudebnaya_statistika/2024/k5_1-svod_vse_sudy-2024.xls/ (дата обращения: 24.07.2025).

смотренную п. «г» ч. 3 ст. 158 УК РФ, за 2024 г. позволяет выделить основные характеристики современного **кибервора**:

– это постоянные жители данной местности – 90,7%; жители иной местности – 9,3%;

– их возраст от 14 до 17 лет – 5,8%; от 18 до 24 лет – 15,7%; от 25 до 29 лет – 13,4%; от 30 до 49 лет – 54,5%; от 50 лет и старше – 10,6%;

– имеют высшее профессиональное образование – 6,1%; среднее профессиональное – 36,8%; среднее общее – 35,2%; основное общее – 21,9%;

– рабочие – 14,8%; государственные и муниципальные служащие – 1,3%; служащие коммерческой или иной организации – 1,7%; лица, осуществляющие предпринимательскую деятельность или участвующие в предпринимательской деятельности, – 1,8%; учащиеся и студенты – 5,3%; нетрудоспособные (неработающие) – 1,2%; трудоспособные лица без постоянного источника дохода – 73,9%¹.

Таким образом, в большинстве случаев киберворы – это трудоспособные, без постоянного источника дохода, постоянные жители данной местности в возрасте от 30 до 49 лет, имеющие среднее профессиональное, среднее общее и основное общее образование.

Из официальных статистических данных МВД России следует, что совершению преступлений в сфере компьютерной информации в большей мере подвержены мужчины, а доля женской преступности в «киберсфере» невероятно мала. Возрастная группа лиц, совершающих киберпреступления, варьируется от 16 до 50 лет².

¹ *Отчет* о демографических признаках осужденных по всем составам преступлений УК РФ. URL: http://www.cdep.ru/userimages/sudebnaya_statistika/2024/k5_1-svod_vse_sudy-2024.xls/ (дата обращения: 24.07.2025).

² *Север Н. С.* Некоторые особенности личности «киберпреступников»: криминологический аспект // Молодой ученый. 2022. № 53. С. 87.

Данные отчета Судебного департамента при Верховном Суде Российской Федерации¹ позволяют выделить следующие основные характеристики современного киберпреступника в сфере компьютерной информации:

- постоянные жители данной местности – 93,8%, жители иной местности – 6,2%;
- их возраст от 14 до 17 лет – 0,43%; от 18 до 24 лет – 49,1%; от 25 до 29 лет – 17,5%; от 30 до 49 лет – 29,6%; от 50 лет и старше – 3,37%;
- имеют высшее профессиональное образование – 27,3%, среднее профессиональное – 43,6%, среднее общее – 21,8%, основное общее – 7,3%;
- рабочие – 21,8%; государственные и муниципальные служащие – 3,8%; служащие коммерческой или иной организации – 41,6%; лица, осуществляющие предпринимательскую деятельность или участвующие в предпринимательской деятельности, – 4,8%; учащиеся и студенты – 3,1%; нетрудоспособные (неработающие) – 0,62%; трудоспособные лица без постоянного источника дохода – 24,9%².

Представленные сведения позволяют сделать вывод, что преступники в сфере компьютерной информации чаще всего являются постоянными жителями данной местности, трудоспособными молодыми людьми в возрасте от 18 до 24 лет, имеющими высшее и среднее профессиональное образование, служащими коммерческой или иной организации.

По данным исследования Group-IB, уже в 2022 г. количество кибератак на российские компании увеличилось почти втрое. Чаще всего (68% от общего числа инцидентов) преступники использовали программы-вымогатели, которые блокируют доступ пользователей к компьютерным системам, и требовали выкуп за его возвращение. Жертвами в основном становились российские ритейлеры, а также

¹ Отчет о демографических признаках осужденных по всем составам преступлений УК РФ. URL: http://www.cdep.ru/userimages/sudebnaya_statistika/2024/k5_1-svod_vse_sudy-2024.xls/ (дата обращения: 24.07.2025).

² Отчет о демографических признаках осужденных по всем составам преступлений УК РФ. URL: http://www.cdep.ru/userimages/sudebnaya_statistika/2024/k5_1-svod_vse_sudy-2024.xls/ (дата обращения: 24.07.2025).

производственные и страховые компании. Ранее хакеры наиболее часто атаковали компании финансового сектора¹.

По данным исследования компании Kaspersky Lab, более 60% киберпреступников в России являются мужчинами в возрасте от 18 до 34 лет. Они обычно занимаются фишингом, разработкой и использованием вредоносных программ и кражей персональных данных².

В качестве примера социально-демографической характеристики киберпреступника в сфере компьютерной информации можно привести данные из судебного решения Преображенского районного суда г. Москвы в отношении гр. С., который, пользуясь своим служебным положением, продавал полученные персональные данные граждан из базы данных ИПС «Следопыт-М», ПТК «Розыск-Магистраль» за определенное денежное вознаграждение, что квалифицируется как неправомерный доступ к охраняемой законом компьютерной информации (ч. 3 ст. 272 УК РФ). Из материалов уголовного дела известно, что гр. С. является гражданином Российской Федерации, с высшим образованием, холостым, не имеющим детей, трудоустроенным, зарегистрированным и проживающим по определенному месту жительства, ранее не судимым, из корыстной заинтересованности, с использованием своего служебного положения (работал в органах внутренних дел) совершил неправомерный доступ к компьютерной информации, что повлекло копирование компьютерной информации³. Изложенное позволяет заключить, что гр. С. обладает всеми указанными выше социально-демографическими качествами киберпреступника в сфере компьютерной информации.

Структуру киберпреступности в Республике Казахстан 89,97% составляет интернет-мошенничество (п. 4 ч. 2 ст. 190 УК РК)⁴.

¹ *Россию захлестнула волна IT-преступлений*. URL: <https://smart-lab.ru/blog/> (дата обращения: 26.11.2023).

² URL: <https://securelist.ru/kaspersky-security-bulletin/> (дата обращения: 26.11.2023).

³ *Приговор* Преображенского районного суда г. Москвы от 14 апреля 2022 г. № 1-363/22 // Судебные и нормативные акты РФ. URL: <https://sudact.ru> (дата обращения: 26.11.2023).

⁴ *Статистические данные* – сведения об уголовных правонарушениях за 2017–2024 годы. URL: <https://qamqor.gov.kz> (дата обращения: 24.07.2025).

Анализ судебной практики позволил ученым составить криминологический портрет киберпреступника в Республике Казахстан, который выглядит следующим образом: мужчины – 78,3%, женщины – 21,7%; лица в возрасте от 21 года до 29 лет – 53,6%, от 29 до 39 лет – 33,53%, в возрасте до 21 года – 12,87%¹.

Среди киберпреступников преобладают представители 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 78,2%, с высшим образованием – 21,8%. На долю безработных приходится 85,2%, отсюда следует, что преступления в основном совершаются лицами с низким уровнем доходов либо не имеющими вообще никаких доходов. Ранее судимыми лицами совершено 38,3% киберпреступлений². Часто киберпреступления совершаются в составе организованной преступной группы³.

Анализ статистической информации за период с 2017 г. по 2024 г. о лицах, совершивших уголовные правонарушения посредством использования телекоммуникационных сетей, в том числе сети Интернет, позволил установить, что лица, совершающие киберхищения в Республике Казахстан, – это, как правило, мужчины, граждане Республики Казахстан, в возрасте от 21 года до 29 лет, в 85% случаев неработающие. При этом в 100% случаев лица, совершающие киберхищения, имеют образование: 15% – высшее, 85% – среднее специальное⁴.

Киберпреступники, совершающие иные уголовные правонарушения в сфере информатизации и связи, – это, как правило, мужчины, граждане Республики Казахстан, в возрасте от 21 года до 39 лет, в 84% случаев неработающие. При этом

¹ Сыздыков А. Ж., Имангалиев Н. К. Криминологический портрет киберпреступника // Наука и жизнь Казахстана. 2018. № 5. С. 58.

² Токанов Е. Е. Криминологический портрет киберпреступника и методы предотвращения преступлений в сфере информатизации и связи. URL: <https://dspace.enu.kz/jspui/bitstream/> (дата обращения: 14.07.2025).

³ См., напр.: Приговор по уголовному делу № 157500121001309 районного суда № 2 Бостандыкского района г. Алматы от 24 января 2017 г. // Банк судебных актов. URL: <https://office.sud.kz/> (дата обращения: 18.11.2023).

⁴ Статистические данные – сведения об уголовных правонарушениях за 2017–2024 годы. URL: <https://qamqor.gov.kz> (дата обращения: 24.07.2025).

в 100% случаев лица, совершающие преступления в сфере информатизации и связи, имеют образование: 17% – высшее, 83% – среднее специальное¹.

В качестве примера социально-демографической характеристики киберпреступника в Республике Казахстан можно привести данные из решения суда Байганинского района Актюбинской области от 10 ноября 2023 г. № 1536-23-00-1/21²: в отношении гр. К. К., 2002 г. р., уроженца Восточно-Казахстанской области, холостого, со средним образованием, безработного, проживающего в г. С., было возбуждено дело об уголовном правонарушении, предусмотренном п. 4 ч. 2 ст. 190 УК РК, в связи с тем, что он с 12 августа по 13 декабря 2022 г., неоднократно обманывая пользователей информационной системы, совершал мошенничество из корыстных побуждений. Вследствие преступления трем потерпевшим причинен значительный материальный ущерб.

Данные из приговора в отношении гражданина К. подтверждают указанные выше социально-демографические качества кибермошенника в Республике Казахстан.

Известны случаи, когда киберпреступник занят на постоянной работе, но при этом совершает кибермошенничество. В качестве примера можно привести приговор Хромтауского районного суда Актюбинской области от 5 января 2023 г. № 1560-22-00-1/81³. В отношении гр. К., 1997 г. р., уроженца Актюбинской области, проживающего по адресу: Актюбинская область, Хромтауский район, работающего в АО горным мастером, ранее не судимого, имеющего среднее образование, холостого, выдвинуто обвинение в совершении уголовного правонарушения, предусмотренного п. 4 ч. 2 ст. 190 УК РК, на основании того, что в августе 2022 г. в городе Х. гр. К., в целях неоднократного совершения хищения чужого имущества путем обмана и злоупотребления доверием пользователей информационной

¹ Там же.

² Приговор суда Байганинского района Актюбинской области в отношении гр. К. от 10 ноября 2023 г. № 1536-23-00-1/21а // Банк судебных актов. URL: <https://office.sud.kz/> (дата обращения: 18.11.2023).

³ Приговор Хромтауского районного суда Актюбинской области от 5 января 2023 г. № 1560-22-00-1/81 // Банк судебных актов. URL: <https://office.sud.kz/> (дата обращения: 18.11.2023).

системы, разместил в мобильном сервисе бесплатных онлайн-объявлений интернет-приложения OLX заведомо ложные объявления о сдаче в аренду жилья в виде квартир в городе и обманным путем завладел денежными средствами девяти потерпевших.

2. Нравственно-психологические качества киберпреступников.

Учитывая мнения ученых и судебную практику Российской Федерации и Республики Казахстан, можно выделить определенные нравственно-психологические качества, которые присущи большинству киберпреступников.

1. Желание легкой наживы. Кибермошенники начинают свою деятельность из-за желания быстро получить деньги. Они ищут уязвимости в системах безопасности и пытаются использовать их для получения финансовой выгоды¹.

2. Низкий уровень эмпатии. Многие киберпреступники не испытывают сочувствия к своим жертвам и не понимают, как их действия могут повредить другим людям². Они часто считают, что потерпевшие сами виноваты в том, что стали жертвами киберпреступности³.

3. Высокий уровень агрессии. Киберпреступники могут проявлять агрессивное поведение как в реальной жизни, так и в онлайн-среде. Они могут использовать киберпреступность как способ проявления своей агрессии и ущемления других людей.

4. Желание получения власти. Киберпреступники могут использовать свои навыки в области кибербезопасности для получения власти и контроля над другими людьми. Они могут использовать свои знания, чтобы взламывать системы и получать доступ к личной информации других людей.

5. Низкий уровень морали. Многие киберпреступники не испытывают чувства ответственности за свои действия и не придерживаются моральных принципов.

¹ Кеуко К. В. Отдельные особенности личности экономического преступника, действующего в сфере электронной коммерции // Право и государство: теория и практика. 2022. № 7. С. 137.

² Pratt T. C., Holtfreter K., Reisig M. D. Routine online activity and internet fraud targeting: extending the generality of routine activity theory // Journal of Research in Crime and Delinquency. 2010. № 47. P. 270.

³ Kshetri N. Cybercrime and cybersecurity in india: causes, consequences and implications for the future // Crime, Law and Social Change. 2016. № 66. P. 315.

пов, могут считать, что законы не применимы к ним и что они имеют право делать все, что хотят¹.

Перечисленные качества не являются универсальными для всех киберпреступников в Российской Федерации и Республике Казахстан, но они часто присущи им. Важно понимать, что киберпреступность представляет серьезную проблему, которая может привести к значительным финансовым и личным потерям для людей, которые становятся ее жертвами. Поэтому необходимо принимать эффективные меры для защиты своих данных и личной информации в онлайн-среде².

Итак, киберпреступники в Российской Федерации и Республике Казахстан часто являются молодыми людьми с определенным уровнем образования, неработающие. Однако нравственно-психологические качества киберпреступников могут быть различными и зависят от конкретной ситуации.

3. Уголовно-правовые качества киберпреступника.

Уголовно-правовые качества личности киберпреступника относятся к набору характеристик, принимаемых во внимание при определении степени виновности лица, совершившего или планирующего совершить киберпреступление³. Перечислим их.

1. Индивидуализм в совершении киберпреступлений. В одиночку были совершены 60% киберпреступлений, в группе или организованной группе – 40% киберпреступлений.

2. Отсутствие криминального опыта. Согласно данным Судебного департамента Российской Федерации преступления в сфере компьютерной информации в подавляющем большинстве случаев совершались осужденными впервые. Ранее судимыми гражданами данные преступления совершались лишь в 7,3% случаев. Ту или иную форму рецидива преступлений в сфере компьютерной информации

¹ *Бегишев И. Р.* Культура информационной безопасности: психолого-правовой аспект // Психология и право. 2021. Т. 11, № 4. С. 208.

² *Молоков В. В.* Киберпреступность: анализ и региональные особенности // Вестник Сибирского юридического института МВД России. 2022. № 4. С. 175.

³ *Долгополов А. А., Ильяшенко А. Н., Белоконов А. В.* Об уголовно-правовых и криминологических аспектах личности преступника и преступного поведения // Вестник Казанского юридического института МВД России. 2024. Т. 15, № 4(58). С. 86–93.

имеют 2,8% осужденных. Статистика рецидивов киберпреступлений или «классических» преступлений у киберпреступников вторит статистике возраста лиц, совершающих противоправные деяния в сфере компьютерной информации, — он сравнительно мал, чтобы успеть стать рецидивистом.

3. Нейтральное отношение к алкоголю и наркотикам. Ни один из осужденных в 2021 г. не совершал киберпреступления под воздействием алкоголя или иных запрещенных веществ¹.

4. Значительность степени тяжести совершенных киберпреступлений. По данным ГИАЦ МВД России, 52,1% киберпреступлений относились к категориям тяжких и особо тяжких². Согласно статистическим данным Республики Казахстан, более 90% уголовных правонарушений, совершенных с использованием информационных технологий, относятся к категории средней тяжести³.

5. Наличие у лиц прямого умысла на совершение киберпреступления и общая направленность преступных киберпосягательств на интересы собственности, получение материальной выгоды.

6. При наличии многообразия способов совершения киберпреступлений приверженность к определенному способу, специализация. Согласно статистической отчетности ГИАЦ МВД России о преступлениях, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, данная группа преступлений совершается с использованием или применением расчетных (пластиковых) карт, компьютерной техники, программных средств, фиктивных электронных платежей, сети Интернет, средств мобильной связи⁴.

Самым распространенным способом совершения интернет-мошенничеств в Республике Казахстан остается онлайн-торговля. Таким способом совершено

¹ Сафин Ф. Ю. О некоторых особенностях личностной характеристики современного киберпреступника // Закон. Право. Государство. 2022. № 4. С. 139.

² Состояние преступности в России за январь–декабрь 2024 г. URL: <http://crimestat.ru/> (дата обращения: 24.07.2025).

³ Статистические данные – сведения об уголовных правонарушениях за 2016–2024 годы. URL: <https://qamqor.gov.kz> (дата обращения: 24.07.2025).

⁴ Состояние преступности в России за январь–декабрь 2024 г. URL: <http://crimestat.ru/> (дата обращения: 24.07.2025).

35,2% интернет-мошенничеств. Как правило, мошенники размещают объявления на сайтах и в социальных сетях. Они указывают заниженные цены за товар или услугу и просят предоплату либо полную оплату¹.

7. Значительность последствий киберпреступлений. В Российской Федерации более 70%, в Республике Казахстан более 93% киберпреступлений совершаются против собственности. Исходя из этого, киберпреступность носит корыстный характер, с чем тесно связан значительный материальный вред, причиняемый киберпреступниками населению. Так, в России размер ущерба, причиненного киберпреступлениями от дистанционных мошенничеств в 2024 г., составил 200 млрд рублей². В Республике Казахстан в 2024 г. подобный ущерб превысил 20 млрд тенге³.

Таким образом, киберпреступник – это человек с высоким уровнем компьютерной грамотности и знаний в области информационных технологий, который использует данные навыки для совершения преступлений. Он представляет значительную угрозу для безопасности в интернете и требует особого внимания со стороны правоохранительных органов⁴.

В рамках проведенного эмпирического исследования были проанализированы приговоры судов Российской Федерации и Республики Казахстан по уголовным делам, связанным с совершением киберпреступлений. Всего в выборку вошло шесть категорий дел: четыре статьи Уголовного кодекса РФ (ст. ст. 158, 159, 159³, 159⁶) и две статьи УК РК (п. 4 ч. 2 ст. 188 и п. 4 ч. 2 ст. 190). Общее число субъектов преступлений, охваченных анализом, составило 150 человек (прил. 6). Анализ гендерного состава показывает выраженное преобладание мужчин среди лиц,

¹ Официальный сайт Министерства внутренних дел Республики Казахстан (МВД РК). URL: <https://www.gov.kz/memleket/entities/qriim> (дата обращения: 24.07.2025).

² В МВД России зафиксировали почти 40%-ный рост суммы ущерба от дистанционных мошенничеств в 2024 г. URL: <https://www.interfax.ru/russia/1009710> (дата обращения: 21.03.2025).

³ Казахстанцы потеряли более 20 млрд тенге из-за интернет-мошенников в 2024 году. URL: <https://24.kz/ru/news/social/691059-kazakhstantsy-poteryali-bolee-20-mlrd-iz-za-internet-moshennikov-v-2024-godu> (дата обращения: 21.03.2025).

⁴ Суходолова Ю. К. Уголовно-правовой аспект учета личности преступников, использующих информационные технологии // Вестник Волгоградского государственного университета. Серия 9, Исследования молодых ученых. 2022. № 20. С. 112.

осужденных за киберпреступления. В РФ мужчины составляют от 63 до 80% (например, по ст. 158 – 72%, по ст. 159 – 78%, по ст. 159⁶ – 80%), в то время как в РК этот показатель достигает 85 и 83% (по ст. 188 – 85%, по ст. 190 – 83%). Таким образом, киберпреступность в обоих государствах в значительной степени характеризуется мужским доминированием, что коррелирует с международными данными по указанной категории преступлений.

Возрастная структура преступников демонстрирует концентрацию в группе 18–35-летних. Так, среди всех категорий дел именно эта возрастная группа составляет абсолютное большинство: в РФ – от 57 до 73%, в РК – до 76%. Лица младше 18 лет представлены крайне незначительно (от 6 до 20% в разных категориях), а доля лиц старше 65 лет отсутствует полностью. Это свидетельствует о том, что основными субъектами киберпреступлений выступают молодые взрослые, обладающие необходимыми цифровыми компетенциями и вовлеченные в цифровую среду.

Уровень образования осужденных характеризуется высокой степенью вариативности, однако доминирующими остаются лица со средним специальным и высшим образованием. В РФ среди субъектов преступлений, предусмотренных ст. ст. 159 и 159⁶, доля лиц с высшим образованием составляет от 20 до 47%, тогда как со средним специальным образованием – от 30 до 53%. Аналогичная картина наблюдается и в РК: среди осужденных по п. 4 ч. 2 ст. 190 УК РК 42% имеют высшее образование, 42% – среднее специальное. Отсутствие образования либо наличие нескольких высших образований фиксируется как исключение. Данный факт указывает на определенную социальную специфику киберпреступности: в отличие от традиционной имущественной преступности, здесь прослеживается участие более образованных и социально активных групп населения¹.

Социально-трудовой статус осужденных демонстрирует значительную долю лиц, не имеющих официального трудоустройства, но при этом обладающих

¹ Пучков Д. В. Киберпреступность как негативное специфическое явление современного общества // Евразийский юридический журнал. 2017. № 12. С. 208.

стабильными источниками дохода. В РФ их доля колеблется от 33 до 53%, а в РК – от 45 до 46%. Лица без постоянного источника доходов составляют от 10 до 25%, а официально трудоустроенные – от 20 до 30%. Это позволяет предположить, что значительная часть субъектов киберпреступлений участвует в теневой экономике или занятиях, неформально приносящих прибыль (например, фриланс, деятельность в даркнете и др.).

Сравнительный анализ позволяет выделить несколько общих тенденций, характерных для обеих стран: доминирование мужчин в структуре субъектов киберпреступлений; преимущественная вовлеченность возрастной группы 18–35 лет; высокая доля лиц с высшим или средним специальным образованием; значительное число лиц с неформальным источником дохода.

Однако в делах, рассмотренных в Республике Казахстан, доля лиц с высшим образованием и официальной занятостью несколько выше, чем в аналогичных делах в РФ. Это может быть связано как с особенностями судебной практики, так и с различиями в структуре преступлений (например, более частое возбуждение дел по признакам мошенничества с применением информационных технологий в банковской сфере).

Проведенное исследование путем анализа приговоров судов РФ и РК по киберпреступлениям (прил. 6) позволило выявить основные криминологические характеристики личности киберпреступника в Российской Федерации и Республике Казахстан, а также выделить социально-демографические, нравственно-психологические, уголовно-правовые качества личности современного киберпреступника, разработать предложения по предупреждению киберпреступности в этих странах¹.

Учитывая большое значение для анализа причин и условий совершения киберпреступлений типичных свойств киберпреступников, считаем актуальной классификацию лиц, занимающихся киберпреступлениями, основанную на степени их вовлеченности в преступную деятельность:

¹ Карабеков К. О., Бабурин В. В. Криминологическая характеристика личности киберпреступника в Российской Федерации и Республике Казахстан // Психопедагогика в правоохранительных органах. 2024. № 1(96). С. 115–118.

1) **начинающие** киберпреступники (51,7%) располагают 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%) имеют средний или выше среднего уровень дохода и 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%) достигли высокого уровня материального благосостояния, находятся в возрасте от 25 до 49 лет. Среди них преобладают мужчины (женщины составляют 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.

Важное значение для организации мер предупреждения двух групп наиболее распространенных киберпреступлений в данных странах имеет знание особенностей личности киберпреступников, в целом характерных для преступников каждой страны. Так, для представителей **первой группы киберпреступлений** в России, с учетом того, что это кибермошенники и киберворы, характерны 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 отноше-

ний с собеседниками. Лица, совершающие кибермошенничества в Казахстане, как правило, мужчины, граждане Республики Казахстан, в возрасте от 21 года до 29 лет, имеющие среднее специальное образование, неработающие. Они в среднем на 15 лет младше, чем российские кибермошенники.

Особенностями лиц, совершающих **киберпреступления в сфере компьютерной информации в России**, являются: желание легкой наживы, преобладание индивидуализма при совершении киберпреступлений, приверженность к определенному способу, специализации в использовании ИТТ при наличии многообразия способов совершения киберпреступлений. Их характеризует 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.

Завершая криминологическую характеристику лиц, совершающих киберпреступления в России и Казахстане, необходимо отметить тот факт, что количество выявленных лиц, совершивших киберпреступления, в общем объеме лиц, совершивших преступления в России, в три раза выше, чем в Казахстане.

ГЛАВА 2. ДЕТЕРМИНАЦИЯ И ПРЕДУПРЕЖДЕНИЕ КИБЕРПРЕСТУПНОСТИ В РОССИЙСКОЙ ФЕДЕРАЦИИ И РЕСПУБЛИКЕ КАЗАХСТАН

§ 1. Детерминанты киберпреступности

Определенные нами ранее закономерности и тенденции киберпреступности позволяют более предметно рассмотреть содержание детерминант киберпреступности в Российской Федерации и Республике Казахстан.

Изучение причин, порождающих преступность, является ключевой проблемой в области криминологии¹. Анализ причин преступности помогает раскрыть ее сущность, объяснить ее происхождение и определить условия и факторы, влияющие на ее существование, что позволяет выявить элементы, способствующие сохранению и возобновлению преступности в настоящее время, а также меры, которые могут быть применены для ее предупреждения².

Анализ причин, условий, факторов и обстоятельств киберпреступности, в частности факторов и обстоятельств отдельных киберпреступлений, требует поиска унифицированного подхода, что имеет важное значение для решения теоретических и практических задач предупреждения киберпреступности в России и Казахстане.

В криминологии принято называть обстоятельства, влияющие на совершение преступления, детерминантами. Понятие «детерминация» происходит от латинского слова *determinare*, что означает «определять». Детерминант обозначает «определитель», детерминировать – «определять, обуславливать», детерминация – «процесс обуславливания, определения».

¹ Лунеев В. В. Курс мировой и российской криминологии : в 2 т. Т. 1 : Общая часть. В 3 кн. Кн. 2 : учебник для магистратуры / В. В. Лунеев. М., 2016. С. 168 ; *Основы криминологии* : учебник / под ред. А. В. Федорова, С. Я. Лебедева. 2-е изд., перераб. и доп. М., 2023. С. 135 ; Джекебаев У. С. Преступность как криминологическая проблема. Алма-Ата, 1974. 128 с.

² Кузнецова Н. Ф., Лунеев В. В. Криминология : учебник. 2-е изд., перераб. и доп. М., 2004. С. 167.

По мнению А. И. Долговой, под детерминизмом понимается признание всеобщей связи и взаимодействия всех объектов, явлений и процессов или «обстоятельств», где последнее используется для объединения понятий причин и условий¹.

На взгляд Л. М. Прозументова, А. В. Шеслера, исследовавших разные подходы к пониманию детерминант преступности в российской криминологии, их полный набор образуют причины, условия и факторы преступности. Очевидно, что выделение указанных детерминант носит условный характер, поскольку в реальной действительности они существуют в тесной взаимосвязи и воплощаются в единую криминогенную социальную ситуацию².

Как полагает В. Н. Комлык, детерминанты – это не только причины, но и те самые обстоятельства, т. е. условия, способствовавшие наступлению последствий, поэтому простое отождествление детерминации и причинности есть ошибка, поскольку причинность выступает одной из форм детерминации³.

Несмотря на существующие исследования, единого мнения у ученых относительно конкретных причин, условий и факторов, способствующих совершению киберпреступлений, на данный момент не сложилось. Добавляет сложности тот факт, что некоторые исследователи классифицируют одни и те же жизненные обстоятельства как причины, в то время как другие относят их к условиям, а третьи рассматривают их как факторы, влияющие на возникновение киберпреступности⁴.

¹ *Криминология* : учебник для вузов / под общ. ред. д-ра юрид. наук, проф. А. И. Долговой. 3-е изд., перераб. и доп. М., 2005. С. 235.

² *Прозументов Л. М., Шеслер А. В.* Некоторые подходы к рассмотрению детерминант преступности в отечественной криминологии // Вестник Томского государственного университета. 2017. № 420. С. 166.

³ *Комлык В. Н.* Значение детерминации преступности в криминологии // Modern Science. 2023. № 12–2. С. 32.

⁴ *Бабурин В. В.* Детерминанты киберпреступлений, совершаемых в сфере экономики // Преступность в сфере экономики: современные тенденции и проблемы противодействия : мат-лы междунар. науч.-практ. конф. Омск, 2022. С. 6 ; *Бабурин В. В., Сурихин П. Л.* Теория причин преступности в российской криминологии: проблемы становления и перспективы развития // Вестник Уральского юридического института МВД России. 2023. № 4. С. 141.

Рассмотрение проблем, причин и условий киберпреступности представляет собой одну из самых сложных задач, противоречиво разрешаемых в глобальной и отечественной науке¹.

Причины, условия и факторы, связанные с киберпреступностью, обусловлены ее специфичностью. Мы считаем, что киберпреступления могут быть результатом не только одной, но и нескольких различных причин.

Исследование причин и условий киберпреступности требует анализа различных факторов. Среди них выделяются система потребностей, интересов, мотивов и ценностей, наличие противоречий между реальными потребностями населения в информационных услугах и возможностью их удовлетворения. Киберпреступления могут быть результатом организованной и профессиональной компьютерной преступности, идеологических и политических мотивов, аномии и отсутствия норм поведения. Имеет большое значение также низкий риск наказания для киберпреступников, что позволяет им действовать безнаказанно. Однако необходимо осознавать, что киберпреступления несут серьезные последствия для общества и экономики, поэтому противодействие им должно стать приоритетом для правоохранительных органов².

Ученые Т. М. Бормотова, А. Е. Ильин, Е. Б. Белянский, В. В. Макаров предлагают разделить причины киберпреступности на социальные, экономические, правовые, организационные и политические³. При этом раскрывают только первые четыре причины. К социальным причинам киберпреступности они относят следующие: 1) широкое использование информационных технологий в обществе и недостаточное соблюдение мер безопасности в соответствии с развитием компьютерных технологий; 2) проблемы с некачественным программным обеспече-

¹ Бугаев В. А., Чайка А. В. Факторы преступности в сфере компьютерных технологий // Ученые записки Крымского федерального университета им. В. И. Вернадского. Юридические науки. 2019. Т. 5, № 4(71). С. 140.

² Карабеков К. О. Причины и условия киберпреступности в Республике Казахстан // Актуальные проблемы профилактики преступлений : мат-лы междунар. науч.-практ. семинара. Омск, 2023. С. 47.

³ Бормотова Т. М., Ильин А. Е., Белянский Е. Б., Макаров В. В. Киберпреступность в России: состояние и методология анализа // Этносоциум и межнациональная культура. 2023. № 10(184). С. 71–72.

нием и несоответствие между потребностями населения в информационных услугах и программном обеспечении и их доступностью из-за низкого уровня жизни; 3) организованный и профессиональный характер киберпреступности.

По мнению Б. М. Ибраевой, одной из социальных причин киберпреступности является стремление хакеров привлечь внимание других людей и компенсировать недостаток общения. Однако это поведение может быть интерпретировано обществом как желание отомстить человечеству за его невежество и изоляцию, хотя это не всегда соответствует правде¹.

В качестве экономических причин Т. М. Бормотова, А. Е. Ильин, Е. Б. Белянский, В. В. Макаров называют: 1) монопольное положение разработчиков программного обеспечения и завышение цен на него; 2) нечестную конкуренцию, вплоть до промышленного шпионажа между производителями программ и антивирусными компаниями; 3) массовое использование вредоносного программного обеспечения; 4) выгодное и относительно безопасное обогащение киберпреступников; 5) возможность легализовать незаконную прибыль.

К правовым причинам указанные ученые относят: 1) неполное международное и национальное законодательство, регулирующие вопросы компьютерных технологий, включая уголовное, гражданское и административное законодательство; 2) высокую задержку в реагировании на новые киберугрозы; 3) недостаточно разработанную концепцию информационной безопасности; 4) отсутствие стандартов безопасности компьютерного программного обеспечения².

В своих научных трудах Н. Л. Коликов обращает внимание на то, что «одной из причин компьютерной преступности являются аномия, слабость норм, отсутствие необходимых нравственных образцов – универсальные стандарты поведения не всегда соответствуют требованиям информационного общества»³.

¹ Ибраева Б. М. Теория цифровой преступности // Интерактивная наука. 2016. № 9. С. 61.

² Бормотова Т. М., Ильин А. Е., Белянский Е. Б., Макаров В. В. Указ. соч.

³ Коликов Н. Л. Причины и условия профессиональной компьютерной преступности // Вестник Южно-Уральского государственного университета. 2011. № 19. Серия «Право». Вып. 26. С. 32.

По мнению К. Н. Евдокимова, причины киберпреступлений играют важную роль, включая недостатки в деятельности правоохранительных органов, занимающихся расследованием киберпреступлений, и слабую организацию работы специалистов в области компьютерных технологий¹.

Позиция И. М. Глотиной заключается в том, что причиной киберпреступности «является незначительный риск: поскольку киберпреступность не имеет геополитических границ, правоохранительным органам трудно ловить преступников, а проведение международных расследований и ведение судебных дел стоят больших денег. Подобные действия, как правило, предпринимаются только в особых случаях»².

Е. С. Айсханова предлагает выделять идеологическую причину совершения киберпреступлений, объясняя это тем, что «подобные виды атак проводятся по этическим, идеологическим или моральным мотивам, направлены на нанесение ущерба или отключение компьютерного оборудования и сетей для выражения недовольства, несогласия действиями и высказываниями отдельных лиц, корпораций, организаций или даже национальных правительств»³.

В продолжение сказанного выше В. Ф. Джафарли предлагает новую перспективу, фокусируясь на понятии «хактивизм», которое относится к использованию компьютерных технологий и информационно-телекоммуникационных сетей, включая интернет, для борьбы за права и свободы личности, такие как свобода слова и информации⁴.

Представляется, что определение основных причин преступности как исходная научная позиция заключается в том, что причина представляет собой явление или группу взаимосвязанных явлений, которые порождают другое явление,

¹ Евдокимов К. Н. Причины компьютерной преступности в современной России // Российский следователь. 2015. № 3. С. 33–37.

² Глотина И. М. Киберпреступность как теневой бизнес // Вестник Челябинского государственного университета. 2016. № 6(388). С. 54.

³ Айсханова Е. С. Причины и мотивы роста киберпреступности как глобального явления современности // Вестник Чеченского государственного университета. 2017. № 4(28). С. 154.

⁴ Джафарли В. Ф. Краткий криминологический анализ причин и условий киберпреступности и методы ее предупреждения // Ученые труды Российской академии адвокатуры и нотариата. 2017. № 2(45). С. 55.

рассматриваемое как следствие или действие. Отмечается, что причины преступности, состоящие из взаимосвязанных явлений, приводят к самой преступности. Однако для наступления конкретного следствия необходимы также конкретные условия. Сами по себе условия не могут вызвать или произвести следствие, но в неких ситуациях или при некоторых обстоятельствах причины способствуют осуществлению действия¹. Проанализировав позиции ученых, мы еще раз убедились в том, что в криминологии отсутствует единое мнение о причинах, условиях, факторах, обстоятельствах преступности.

Исходя из целей и задач нашего исследования, мы считаем необходимым выделять две группы основных детерминант киберпреступности в Российской Федерации и Республике Казахстан: это внутренние и внешние детерминанты. При этом каждая из основных групп детерминант имеет свои подгруппы детерминант, отражающие специфику действия факторов, обуславливающих совершение киберпреступлений, связанных с основными сферами жизнедеятельности общества и способами их влияния на общество. Так, в рамках основной группы внутренних детерминант, с учетом специфики жизнедеятельности общества, необходимо выделять социально-экономические, организационно-технические, правовые, организационно-управленческие детерминанты. В рамках основной группы внешних детерминант, с учетом внешнего воздействия на общество, необходимо выделять активные и пассивные детерминанты².

В целях изучения общественного мнения относительно причин совершения киберпреступлений нами были опрошены граждане Российской Федерации (434 человека; охват территории составил города Омск, Барнаул, Красноярск, Санкт-Петербург, Москва) (прил. 1) и Республики Казахстан (прил. 2) (320 человек; охват территории составил города Астана, Алматы, Караганда, Актобе, Талдыкорган).

¹ *Кобец П. Н.* Киберпреступность: современные виды, причины, ее порождающие, и особенности предупреждения // Вестник Самарского юридического института. 2022. № 1(47). С. 52.

² *Карабеков К. О.* Детерминанты и меры предупреждения киберпреступлений в Российской Федерации и Республике Казахстан // Евразийский юридический журнал. 2025. № 7. С. 356.

На вопрос «Что, по Вашему мнению, является причиной совершения киберпреступлений?» респонденты ответили: низкий уровень дохода – 59,90%; анонимность в сети Интернет – 48,84%; несовершенство законодательства в этой сфере – 39,86%; низкий уровень культуры – 30,41%; безработица – 19,81%; ненависть и агрессия – 11,98% (прил. 1 и 2). Из этого следует, что основная причина киберпреступности заключается в том, что киберпреступники, воспользовавшись анонимностью в киберпространстве, стараются заработать «легкие деньги».

По статистике, более 70% общей преступности состоит из преступлений против собственности. Поэтому в связи с развитием информационно-телекоммуникационных технологий у преступников появились новые условия совершения преступлений в киберпространстве.

Учитывая расхождения в мнениях ученых относительно содержания причин, условий и факторов, обуславливающих существование киберпреступности, считаем необходимым при характеристике детерминант исходить из фактического содержания киберпреступности в России и Казахстане, как киберпреступности корыстной направленности. С этой целью нами было изучено содержание внутренних и внешних детерминант корыстной киберпреступности.

Рассмотрим выделенные нами в первой группе социально-экономические, организационно-технические, организационно-правовые, организационно-управленческие подгруппы детерминант подробнее.

Социально-экономические детерминанты связаны с широким использованием информационно-коммуникационных технологий в обществе, а также сосредоточением в сети Интернет большого количества персональных данных граждан наших стран.

С одной стороны, процесс цифровизации значительно ускоряет передачу информации, предоставление различных услуг и трудовую деятельность. С другой – этот процесс также способствует увеличению количества преступле-

ний, связанных с мошенничеством в онлайн-пространстве¹. При использовании маркетплейсов для проведения платежей необходимо предоставлять личные данные банковских карт, которые затем остаются в цифровом виде на компьютерах и гаджетах. Это открывает злоумышленникам доступ к электронно-вычислительной технике и позволяет использовать полученную информацию для совершения незаконных финансовых операций.

Считаем, 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.

Базовым условием роста киберпреступности в указанных странах выступает развитие цифровых финансовых услуг. В Казахстане за условную точку отсчета диджитализации потребительских финансовых услуг можно взять запуск мобильного приложения Kaspi, который состоялся в июне 2017 г.² Появление мобильного приложения Kaspi стало определяющим фактором для казахстанского рынка финансовых услуг. В результате уже сегодня владелец мобильного телефона может оформить кредит, открыть депозит, провести сделку на фондовом рынке, заказать товар, оплатить штраф, получить государственную услугу и даже разместить объявление о продаже, не отрываясь от экрана.

В свете растущей популярности этого нового продукта некоторые игроки решили повторить успех первопроходца, запустив аналогичные приложения, в то время как другие занялись цифровизацией ипотеки, автокредитов и брокерских операций.

Для визуализации действий держателей банковских карточек мы рассмотрим соответствующую статистику Национального банка Республики Казахстан за

¹ Репецкая А. Л. Современное состояние, структура и тенденции российской преступности // Вестник Омского университета. Серия «Право». 2018. № 1(54). С. 155 ; Пинкевич Т. В. Цифровое неравенство как фактор преступности // Виктимология. 2024. Т. 11, № 4. С. 544.

² URL: <https://kz.kursiv.media/chto-stalo-prichinoj-rosta-kiberkriminala-v-kazahstane/> (дата обращения: 31.01.2024).

первые полгода 2017 г.¹ Как следует из цифровых показателей, жители Казахстана обычно снимают наличные деньги с помощью банкоматов в двух случаях из трех. Что касается суммы наличных переводов, то их доля в значительной степени преобладала, поскольку каждые шесть тенге из семи снимались с помощью банкоматов. Оставшаяся сумма денег на карточках была использована в основном для безналичных платежей. Однако большая часть этих платежей представляла собой оплату товаров и услуг банковской карточкой, что не является продуктом финтех.

Цифровизация многих банковских услуг изменила поведение держателей карточек в Казахстане. Статистика национального банка по платежным карточкам указывает на то, что, во-первых, граждане Казахстана, использующие банковские карточки, в 29 раз чаще совершали безналичные платежи, чем снимали наличные деньги в банкомате, а количество безналичных транзакций в четыре раза превышало сумму денег, снятых в банкоматах; во-вторых, кардинально изменилась среда безналичных платежей: две из трех безналичных транзакций совершаются в интернете, включая мобильный банкинг, а из семи тенге, отправленных в безналичной форме, шесть – в интернете и благодаря мобильному банкингу; в-третьих, почти в двадцать пять раз вырос объем электронной розничной коммерции (с 106,9 млрд тенге в 2017 г. до 2,7 трлн тенге по итогам 2024 г.)².

Удобство использования и свободный доступ к онлайн-технологиям из дома также являются факторами, способствующими совершению киберпреступлений. Такие преступления в основном совершаются без выхода из дома. Преступники могут обогащаться, не отходя от компьютера или ноутбука. При этом далеко не всем преступникам требуется обладать высоким уровнем образования, навыков и знаний в области программирования. Часто достаточно владеть навыком осуществления нескольких операций посредством специальных мобильных приложений на телефонах и смартфонах, чтобы украсть деньги со счета жертвы.

¹ URL: <https://www.nationalbank.kz/ru> (дата обращения: 31.01.2024).

² Данные Бюро нацстатистики АСПР РК. URL: <https://kapital.kz/finance/77204/chego-ozhidat-na-rynke-beznalichnykh-platezhey.html/> (дата обращения: 23.02.2025); URL: <https://zhanalyk.kz/rost-elektronnoi-kommertsii-v-kazakhstane-dostig-29-za-god/> (дата обращения: 23.02.2025).

Например, в 2018 г. гр. Ф. смогла похитить деньги с банковского счета своего отца при помощи системы дистанционного банковского обслуживания через его мобильный телефон. Общая сумма похищенных средств составила 20 800 рублей; ключевую роль в данной ситуации сыграло существование упрощенного метода банковских операций с помощью мобильных приложений¹.

Развитие информационных технологий приводит к увеличению доступности сети Интернет. Факт увеличения доступности сети Интернет подтверждается результатами проведенного нами анкетирования. На вопрос «Какими источниками Вы пользуетесь для получения информации об актуальных новостях?» 52,76% респондентов обеих стран отметили новостные сообщества в социальных сетях и мессенджерах (в том числе неофициальные СМИ); 39,86% указали веб-сайты и мобильные приложения официальных СМИ; 7,37% назвали телевидение и печатные издания (прил. 1 и 2). Развитие информационных технологий создало благоприятные условия для совершения киберпреступлений, которым мы должны научиться противостоять.

Внешние социальные процессы влияют на совершение преступлений. Ю. А. Мерзлов выделяет ряд условий, способствующих совершению киберпреступлений: быстрое развитие сферы высоких технологий и широкое распространение компьютерной техники среди населения, влияние семейного и внесемейного окружения на процесс становления личности правонарушителя в сфере компьютерной информации, наличие специальностей в высших образовательных учреждениях, по которым ведется подготовка обучающихся с привитием им профессиональных знаний, умений и навыков программирования².

Социально-психологические процессы в сознании и поведении киберпреступника играют ключевую роль в формировании и поддержании их криминального поведения в сети. По нашему мнению, социально-психологические процес-

¹ Постановление Елабужского городского суда по уголовному делу № 1-58/2019 от 18 января 2019 г. // Сайт судебных и нормативных актов. URL: <https://sudact.ru/regular/doc/> (дата обращения: 19.01.2024).

² Мерзлов Ю. А. Криминологический портрет лиц, совершающих преступления в сфере компьютерной информации // Правопорядок: история, теория, практика. 2015. № 4(7). С. 56–61.

сы, которые происходят в сознании и поведении киберпреступника, связаны с его отношениями с другими людьми, социальными стереотипами, ценностями и мотивациями. Они включают в себя такие аспекты, как:

1. Мотивация: киберпреступники могут быть мотивированы различными факторами (например, желанием заработать деньги, установить контроль над другими людьми, причинить вред или просто испытать ощущение власти).

2. Социальные стереотипы: киберпреступники могут быть подвержены влиянию, общественным установкам и стереотипам, в которых они убеждены, могут верить, что жертвы заслуживают того, что с ними происходит, или что их действия оправданы нормами определенной группы или идеологии.

3. Восприятие мира: киберпреступники могут иметь искаженное восприятие реальности, агрессивные или параноидальные установки, что влияет на их поведение и оценку возможных последствий своих действий.

4. Эмпатия и социальное понимание: у киберпреступников может быть ограниченное восприятие и понимание эмоций и потребностей других людей, приводящие к пренебрежительному или жестокому поведению в сети.

5. Групповая динамика и социальные связи: киберпреступники могут быть вовлечены в интернет-группы или сообщества, где они находят социальную поддержку, советы и подтверждение своих действий, что оказывает сильное влияние на их поведение и решения.

Одной из главных причин, заставляющих людей совершать киберпреступления, является преследование корыстной цели¹. Современные технологии и доступ к интернету предоставляют возможность людям совершать различные преступления для личного обогащения. В этом процессе имеют значение наличие финансовых обязательств и сложное финансовое положение, которое требует дополнительных денежных средств, доступных через совершение киберпреступлений².

¹ Простосердов М. А. Экономические преступления, совершаемые в киберпространстве, и меры противодействия им : дис. ... канд. юрид. наук. М., 2016. С. 145.

² Семь безопасных информационных технологий / А. С. Марков, А. В. Дорофеев, А. В. Барабанов, В. А. Цирлов. М., 2017. С. 185.

По итогам анкетирования населения Российской Федерации и Республики Казахстан выявлено, что 78,80% респондентов столкнулись с фактом интернет-мошенничества (прил. 1 и 2).

В 2017 г. было совершено преступление в целях хищения денежных средств. Злоумышленник смог проникнуть в корпус банкомата одного из банков и успешно подключиться к системному блоку. При помощи специального вредоносного программного обеспечения он обошел все меры защиты и без всяких затруднений получил доступ к денежным средствам. Кроме того, выплатил вознаграждение соучастнику, разработавшему данное вредоносное программное обеспечение. Подсудимый А. свою вину в инкриминируемых ему преступлениях признал полностью и пояснил, что осенью 2016 г. он искал в интернете способ заработка из-за финансовых проблем, зашел на сайт по поиску работы, на форуме познакомился с мужчиной, который представился Н. и рассказал ему о возможности заработать не менее 40 000 рублей в месяц¹.

Другой случай – подсудимый О., нигде не работая и нуждаясь в денежных средствах, в поисках путей легкого материального обогащения решил встать на путь совершения преступлений, направленных на хищение денежных средств, путем обмана и злоупотребления доверием граждан. Для воплощения в реальность преступного умысла он стал искать пути улучшения своего статуса в обществе, необходимого для быстрого получения доверия перед людьми, и создал страничку в социальной сети Facebook² и на интернет-сайтах OLX.kz и home-mebel, далее стал распространять о себе информацию, что он занимается изготовлением корпусной мебели для квартир и домов. Впоследствии решил незаконно обогатиться путем полного неисполнения или частичного исполнения взятых на себя обяза-

¹ Приговор по делу № 1-192/2017 от 18 сентября 2017 г. Октябрьского районного суда г. Самары (Самарская область). URL: <https://sudact.ru/regular/> (дата обращения: 24.01.2024).

² Принадлежит компании Meta, деятельность которой признана экстремистской и запрещена на территории Российской Федерации.

тельств перед клиентами, тем самым улучшив свое положение, завуалировав данные обстоятельства гражданско-правовыми отношениями¹.

Представленные примеры ярко демонстрируют корыстные мотивы киберпреступников, побуждающие их совершить преступление в целях улучшения своего материального благосостояния.

По данным Судебного департамента при Верховном Суде Российской Федерации о демографических признаках, около 47% осужденных за киберпреступления – трудоспособные лица без постоянного источника дохода². В Республике Казахстан на долю безработных приходится 82,3% киберпреступлений, что позволяет судить о том, что киберпреступления в основном совершаются лицами, имеющими низкий уровень доходов либо не имеющими никаких доходов³.

«В некоторых случаях моделируемый результат может быть не связан с извлечением дохода (месть, приобретение или укрепление авторитета, дискредитация кого-либо, “альтруизм”). Киберпреступниками могут преследоваться политические цели»⁴. Такое возможно при совершении преступлений, связанных с экстремизмом или терроризмом, а также при совершении киберпреступлений, направленных против государственной власти и основ государственного строя. Учитывая вышесказанное, предполагаем, что совершение киберпреступлений может быть обусловлено желанием киберпреступников подчеркнуть свой статус в криминальном мире и проявить свою неординарность.

На основе исследования судебных дел было выявлено, что именно корысть и месть побуждают людей к совершению подобных преступлений. Например, в Липецке произошло следующее преступление: женщина, ранее работавшая

¹ Приговор районного суда № 2 Бостандыкского района г. Алматы Республики Казахстан от 16 августа 2021 г. № 7550-21-00-1/243 в отношении О. URL: <https://sud.gov.kz/rus/bank> (дата обращения: 24.01.2024).

² Отчет о демографических признаках осужденных по всем составам преступлений УК РФ. URL: https://www.cdep.ru/userimages/sudebnaya_statistika/ (дата обращения: 09.02.2024).

³ Токанов Е. Е. Криминологический портрет киберпреступника и методы предотвращения преступлений в сфере информатизации и связи. URL: <https://dspace.enu.kz/jspui/bitstream/> (дата обращения: 24.01.2024).

⁴ Тулегенов В. В. Киберпреступность как форма выражения криминального профессионализма // Криминология: вчера, сегодня, завтра. 2014. № 2(33). С. 94–97.

в частной компании, воспользовалась своим доступом к корпоративной электронной почте, чтобы отомстить своему бывшему работодателю за увольнение. Она незаконно взломала почтовый ящик фирмы и сменила логин и пароль, чтобы лишить всех возможности получить к нему доступ¹.

Одна из причин, объясняющих преступное поведение киберпреступника, – личные враждебные отношения. Например, в 2019 г. был вынесен приговор в отношении В., которая из-за личной неприязни к своей коллеге, работая в офисе продаж мобильного оператора, злоупотребляла своими полномочиями. Она изменила данные sim-карты пострадавшей, чтобы получить доступ к ее конфиденциальной информации, размещенной в социальных сетях. Кроме того, она загрузила на страницу потерпевшей интимные фотографии².

Иногда преступное поведение людей, осуществляющих атаки с использованием компьютерных технологий, обусловлено неприязнью, враждой или унижением человеческого достоинства. Чаще всего такие преступления наблюдаются в случаях, когда экстремисты используют интернет для осуществления своих действий. В 2018 г. М. был признан виновным в размещении на своей странице в социальной сети материалов, которые целенаправленно возбуждали ненависть, вражду и унижение представителей различных национальностей, происхождения, религиозных взглядов и социальных групп. В числе целей М. были представители определенных национальностей, иудеи, банкиры международного уровня, представители государственной власти Российской Федерации и СССР, а также Президент Российской Федерации и его сторонники³. Молодой человек объяснил, что его действия были результатом замешательства и недопонимания текущих собы-

¹ *Постановление* Советского районного суда г. Липецка Липецкой области по уголовному делу № 1-523/2019 от 10 декабря 2019 г. // Сайт судебных и нормативных актов. URL: www.sudact.ru/regular/doc/E6nii5VI82NS (дата обращения: 24.01.2024).

² *Приговор* Бугурусланского районного суда Оренбургской области по уголовному делу № 1-149/2019 от 18 июля 2019 г. // Сайт судебных и нормативных актов. URL: www.sudact.ru/regular/doc/ (дата обращения: 24.01.2024).

³ *Приговор* Сыктывкарского городского суда Республики Коми по уголовному делу № 1-710/2018 от 22 ноября 2018 г. // Сайт судебных и нормативных актов. URL: www.sudact.ru/regular/doc/t3IB9ntfbkQC (дата обращения: 24.01.2024).

тий. По его словам, люди с радикальными взглядами оказали на него давление, что могло спровоцировать угрозу устоявшемуся общественному порядку.

Опытные IT-специалисты и программисты, в отличие от новичков, которые часто поддаются внешнему воздействию, обычно объясняют свое участие в киберпреступлениях желанием испытать собственные технические компетенции и профессиональные качества через выполнение кибератак.

В 2017 г. гр. С., окончивший государственное образовательное учреждение среднего профессионального образования по специальности «программист», являясь опытным пользователем компьютерных систем и обладая обширными знаниями в сфере IT, из личных побуждений, обусловленных желанием проверки своих способностей и знаний в области информационных технологий в целях самоутверждения, совершил умышленное преступление, связанное с использованием компьютерной программы, заведомо предназначенной для несанкционированной нейтрализации средств защиты компьютерной информации¹. Используя свои продвинутое технические умения, он смог обойти системы безопасности незамеченным, добраться до серверов региональных министерств и ведомств на Дальнем Востоке.

По мнению К. Н. Евдокимова, «одной из таких причин (причины, которые не имеют личной или корыстной мотивации, но затрагивают интересы определенной группы лиц. – К. К.) является наличие противоречия между реальными потребностями населения в информационных услугах, программной продукции и возможностью их удовлетворения реальными способами в силу низкого уровня жизни»², а один из аспектов, который способствует совершению киберпреступлений, – это организованный и профессиональный характер компьютерной преступности.

¹ Постановление Южно-Сахалинского городского суда Сахалинской области по уголовному делу № 1-908/2019 от 15 августа 2019 г. // Сайт судебных и нормативных актов. URL: www.sudact.ru/regular/doc/6ywo62uBMgoC (дата обращения: 24.01.2024).

² Евдокимов К. Основные причины компьютерной преступности в современной России // The Journal of Siberian and Far Eastern Studies. 2015. № 8. С. 64.

Такое поведение киберпреступникам позволяет ощущать себя единой группой преуспевающих людей, принадлежащих к социальной элите, научно-техническому андеграунду и подтверждать свой особый статус в мире криминала. Это происходит, когда некоторые люди имеют доступ к определенным возможностям, в то время как другие их лишены. В данном случае речь идет о высокой стоимости лицензионных программных продуктов и низкой заработной плате населения, что делает эти продукты недоступными для пользователей компьютеров. В свою очередь, это приводит к росту спроса на нелегальные компьютерные программы. История судебных прецедентов знает случаи, когда указанные лица совершали различные преступления, связанные с установкой на компьютеры клиентов нелегальных программ, таких как ArchiCAD, AutoCAD, Microsoft Windows, Компас, 1С и др.

Например, через сайт «Авито» один предприниматель искал клиентов, которым за определенную плату предлагал установку программных продуктов Microsoft Windows 10 Professional и Microsoft Office Standard 2010 с помощью своей флэш-карты. Для этого он также использовал компьютерные программы, предназначенные для обхода средств защиты информации указанных программных продуктов. Такие преступления характеризуются профессиональным подходом, узкой специализацией, наличием конкретных навыков и соответствующего образования, систематическим получением прибыли и т. д. Не имея других возможностей для легального заработка, эти лица используют свои интеллектуальные способности для совершения киберпреступлений в области компьютерной информации. В редких случаях причиной подобных преступлений может быть отсутствие желания указанного субъекта заниматься честным трудом или выполнением другой тяжелой или низкооплачиваемой работы¹.

Организационно-технические детерминанты: низкий уровень осведомленности о правилах использования интернет-ресурсов, недостаточное внимание

¹ Постановление Комсомольского районного суда г. Тольятти Самарской области по уголовному делу № 1-269/2019 от 9 декабря 2019 г. // Сайт судебных и нормативных актов. URL: www.sudact.ru/regular/doc/ (дата обращения: 03.01.2024).

руководства организаций к проблеме информационной безопасности, некомпетентность и невысокая квалификация специалистов организации и сотрудников правоохранительных органов в области кибербезопасности, слабая защита информационных систем, уязвимость программного обеспечения, отсутствие эффективных механизмов контроля и обнаружения кибератак.

Низкий уровень осведомленности о правилах использования интернет-ресурсов является еще одним детерминантом киберпреступности. Люди, предоставляющие свои личные данные или информацию, которая может быть использована против них без их согласия, могут быть подвергнуты потенциальной опасности, что может привести к ущемлению чести и достоинства пользователей, а также к распространению их личных данных. Пользователи интернета, минуя этап ознакомления с правилами конкретного сервиса, добровольно размещают компрометирующую информацию о себе. Злоумышленники, идентифицируя таких людей, вымогают у них деньги, угрожая распространить полученные сведения. Большинство неподготовленных людей готовы подчиниться вымогателям. Многие преступления такого рода остаются латентными, поскольку вымогатели используют фейковые аккаунты и требуют перевода денежных средств через электронные платежные системы, такие как биржи криптовалют, чтобы оставить меньше цифровых следов.

Отсутствие эффективного и надежного механизма защиты информационных систем, таких как брандмауэры, антивирусы, системы обнаружения вторжений (IDS) и предотвращения вторжений (IPS), делает их более уязвимыми для кибератак и позволяет злоумышленникам получать несанкционированный доступ к системе или информации.

Уязвимости программного обеспечения могут быть использованы злоумышленниками для внедрения в системы или получения доступа к конфиденциальной информации. Уязвимости могут возникать из-за ошибок в коде программы, отсутствия обновлений или патчей безопасности, слабых паролей и других факторов. Недостаточная кибербезопасность может быть следствием уязвимости в системах и программном обеспечении, а также отсутствия эффективной защиты

информации. В январе–мае 2023 г. продажи потребительских антивирусов в России составили 195 тыс. лицензий, что на 61% меньше, чем годом ранее¹. В Казахстане почти все компании используют антивирусное программное обеспечение, однако 21% из них не следит за новыми киберугрозами². Вместе с тем при анкетировании 100% респондентов отметили, существует обязательная необходимость использования антивирусных программ (прил. 1 и 2).

Что касается отсутствия эффективных механизмов контроля и обнаружения атак, то недостаточное внимание к контролю и обнаружению атак может привести к непродолжительности кибератаки или даже к невозможности обнаружения инцидента вообще. Наличие средств мониторинга, регистрации и анализа сетевого трафика, системы регистрации аудита и инцидентов, а также имеющийся обученный и компетентный персонал, способный оперативно обнаруживать потенциально вредоносную активность, представляются важным фактором в предотвращении и выявлении киберпреступления.

К сожалению, квалифицированные IT-специалисты в определенных случаях могут перейти на «темную» сторону и использовать свои навыки для незаконных целей. В Российской Федерации спрос на IT-специалистов за год вырос: в сентябре 2022 г. на портале hh.ru было открыто 64 тыс. вакансий, а в сентябре 2023 г. компании разместили 76 тыс. вакансий. Согласно статистике hh.ru, годовой прирост подобных вакансий составил 18%³. В Республике Казахстан за последние четыре года количество вакансий по профессиональной области «Информационные технологии, интернет, телеком» увеличилось на 88,5%⁴. Получается, что спрос на IT-специалистов высокий, но при этом они особо не ищут постоянную работу.

Следует отметить, что, помимо высшего или среднего специального образования, молодые киберпреступники часто приобретают соответствующие компьютерные навыки самостоятельно в сети Интернет, через профессиональные форумы

¹ URL: <https://www.tadviser.ru/index.php/> (дата обращения: 22.01.2024).

² URL: <https://informburo.kz/novosti/uroven-zarazheniya-kibervirusami-v-kazahstane-8-v-ssha-i-yaponii-on-nulevoy.html/> (дата обращения: 22.01.2024).

³ URL: <https://habr.com/ru/articles/770720/> (дата обращения: 22.01.2024).

⁴ URL: <https://kapital.kz/tehnology/107740/top-10-vostrebovannykh-it-spetsialistov-v-kazahstane/> (дата обращения: 22.01.2024).

или сайты, где публикуются различные способы и механизмы работы с компьютерными технологиями и информационными ресурсами. Очевидно, что наличие различных доступных программ и языков программирования имеет огромное значение, так как они позволяют создавать вредоносные программы, программы-взломщики и другие инструменты, необходимые для совершения киберпреступлений. Кроме того, в интернете можно найти специализированное программное обеспечение как за определенную денежную сумму, так и бесплатно. Известная практика хакерства и широкое распространение цифровых технологий вызвали интерес у молодого поколения. Популярным стало углубляться в компьютерные и игровые интересы, изучать все возможные детали о компьютерах, мобильных устройствах и других гаджетах, а также об интернет-технологиях. Модным стало объединяться в различных форумах и социальных сетях по компьютерным и игровым интересам. Например, существует форум darkmoney.cc, где обычные киберпреступники могут получить информацию о способах совершения различных преступлений. В 2015 г., гр. З., имеющий знания в области компьютерной информации и техники, познакомился на форуме darkmoney.cc с неизвестным лицом, от которого узнал о специальных программах для мобильных телефонов, способных без ведома пользователя «зараженного» устройства совершать кражи денежных средств с открытых счетов в ПАО «Сбербанк» с помощью sms-сообщений. После этого З. и его соучастники, используя специализированное взломанное программное обеспечение, смогли совершить 12 краж денежных средств на сумму свыше 90 тыс. рублей¹.

Данные знания могут послужить как во благо людей, общества и государства, так и во вред им, позволяя совершать преступления с использованием компьютерных технологий. Как показывает судебная практика, такие знания и умения требуются молодым специалистам при совершении хакерских атак на различные сайты и интернет-порталы.

¹ Приговор Заельцовского районного суда г. Новосибирска Новосибирской области по уголовному делу № 1-158/2017 от 13 ноября 2017 г. // Сайт судебных и нормативных актов. URL: www.sudact.ru/regular/ (дата обращения: 23.01.2024).

В качестве дополнительной детерминанты можно выделить низкий уровень информационной грамотности населения: слабое понимание основных принципов работы с информацией и технологиями, ограниченный навык управления персональными данными и защиты конфиденциальной информации, уязвимость перед кибератаками и мошенничеством, включая фишинг, перехват данных и кражи личной информации¹.

По итогам анкетирования населения Российской Федерации и Республики Казахстан выявлено, что 79,95% респондентов подтверждают опасность в сети Интернет, но для 20,04% опрошенных пользование интернетом не вызывает никакой опасности (прил. 1 и 2).

Недостаточная осведомленность о проблемах кибербезопасности и понимание рисков киберпреступности в обществе создают благоприятное окружение для киберпреступников. Недостаток знаний о мероприятиях по кибербезопасности может привести к уязвимостям, например, путем совершения незащищенных онлайн-платежей или раскрытия личной информации. 57,1% опрошенных не знают официальных интернет-ресурсов, куда можно отправить информацию о факте мошенничества в сети Интернет (номер телефона, откуда звонили, адрес или название сайта и др.) (прил. 1 и 2).

Недостаточное внимание руководства организаций к проблеме кибербезопасности: отсутствие приоритета, отведенного кибербезопасности в планах и бюджетах организаций, может привести практически к игнорированию проблем кибербезопасности и неправильному распределению ресурсов. Непринятие стратегических и организационных мер по защите информации сотрудников также может влиять на уязвимость конфиденциальной информации.

Некомпетентность и низкая квалификация специалистов организации и сотрудников правоохранительных органов в области кибербезопасности заключаются в отсутствии актуальных знаний о новейших технологиях и средствах за-

¹ Родина Е. А. Противодействие криминальной виктимизации пользователей сети «Интернет» в киберпространстве : дис. ... канд. юрид. наук. Саратов, 2022. С. 140.

щиты, неполном понимании рисков и угроз, связанных с кибербезопасностью, ограниченных навыках в решении сложных проблем, вызванных кибератаками.

Результаты исследования выявили дополнительные условия, способствующие совершению киберпреступлений. Одним из таких условий является слабая защищенность баз данных, облегчающая несанкционированный доступ к персональным данным абонентов и клиентов, а также уязвимость некоторых цифровых технологий, включая систему передачи сообщений и потоковой информации. Существование таких уязвимостей в значительной степени облегчает преступникам доступ к необходимой информации и другим данным.

К указанным условиям следует отнести и несовершенство парольной системы компьютерных технологий, предназначенной для защиты от несанкционированного доступа. Такую систему легко подвергнуть «взлому» с применением специальных «кодов-грабберов», «патчей» и прочих нелегальных программ.

Технология «умных» домов и «умных» городов с бесчисленными камерами видеонаблюдения является новым условием, способствующим совершению преступлений в сфере компьютерной информации. Вступление таких технологий в нашу жизнь направлено на создание комфортных условий для проживающих и облегчение повседневной жизнедеятельности, включая обеспечение безопасности населения. Тем не менее, как и у любых других технических разработок, существует обратная сторона этого явления.

«В перспективе такие технологии „умных“ городов, как управление дорожным движением и освещением, камеры контроля скорости, системы общественного транспорта и электроснабжения, а также инфраструктура управления воздушным движением и т. д., станут популярной мишенью для хакеров»¹.

То же самое можно сказать и о концепции «умного» дома, где разнообразные устройства и гаджеты, обладающие камерами и доступом в интернет, могут использоваться не только во благо владельцев дома, но и в интересах киберпреступников. Более того, многие из таких устройств содержат значительное количе-

¹ Пучков Д. В. Основные тенденции развития международной преступности в сфере реализации кибертехнологий // Общество и право. 2019. № 2(68). С. 41–45.

ство программных ошибок и уязвимостей. Аналогичная проблема прослеживается в социальных сетях и электронных мессенджерах. Все эти уязвимости могут быть использованы киберпреступниками для достижения собственных целей, включая причинение вреда потерпевшим.

«Хакерские атаки» на интернет-порталы учреждений, находящихся в других городах, стали второй особенностью преступных действий. Объекты для кибератак выбираются случайно. Эти преступления остались бы нераскрытыми, если бы киберпреступники не были выявлены и привлечены к уголовной ответственности вовремя. Анонимность в киберпространстве признается одним из важных факторов для таких преступлений в сфере компьютерной информации.

«Взломщики маскируются с использованием вымышленных учетных записей, многочисленных идентификаторов пользователя, фальшивых мандатов, запутанных свойств файлов, сложной зашифровки, прокси-серверов, виртуальных частных сетей и возможности маскировать атаки в глобальном киберпространстве»¹.

Такое условие содействует укрыванию киберпреступниками своих преступлений, в результате чего возникают безнаказанность и неограниченность противоправных действий, так как правоохранительным органам не всегда удастся раскрыть подобные преступления.

В 2018 г. студент 2-го курса заочной формы обучения решил провести проверку своих компьютерных знаний, занимаясь взломом интернет-ресурсов. Он использовал специальную компьютерную программу под названием SQLi Dumper, которая предназначена для обхода систем защиты компьютерной информации через использование метода SQL-инъекций². В результате студент смог

¹ *Старкин С. В.* Кибербезопасность и киберреволюция: критический анализ базовых концептов // Вестник Московского университета. Серия 12, Политические науки. 2015. № 1. С. 35–53.

² SQL-инъекция – это один из самых доступных способов взлома сайта. Суть таких инъекций – внедрение в данные (передаваемые через GET, POST-запросы или значения Cookie) произвольного SQL-кода. Если сайт уязвим и выполняет такие инъекции, то по сути есть возможность делать с базами данных (чаще всего это MySQL) все, что угодно (*SQL-инъекции. Проверка, взлом, защита.* 20.10.2011. URL: <https://habr.com/ru/post/130826> (дата обращения: 16.01.2024)).

«взломать» интернет-ресурс, принадлежащий Государственному бюджетному учреждению культуры «Государственный историко-архитектурный художественный и ландшафтный музей-заповедник „Царицыно“»¹.

Аналогичным образом, путем синтаксических подстановок (переборов) логических структур языка SQL, с использованием операторов AND, OR, UNION ALL и функции CONCAT в кодировке URL, жителем г. Ангарска был осуществлен взлом информационного портала ФГБУН «Институт физики полупроводников им. А. В. Ржанова» СО РАН, расположенного в г. Новосибирске².

В обоих случаях «хакеры» применили знания и квалификацию в области взлома веб-сайтов, полученные из Интернета. Благодаря Всемирной сети они обнаружили и получили доступ к программам, основанным на декларативном языке программирования SQL, необходимым для выполнения взлома сайтов.

Организационно-правовые детерминанты. С правовой точки зрения 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.

О. Н. Головинов и А. В. Погорелов по этому поводу пишут, что «несовершенство законодательства приводит к отсутствию на национальном уровне механизма регистрации жалоб населения на кибермошенничество... отсутствует законодательный механизм ответственности производителей программного обеспечения перед своими клиентами, так как предлагаемые продукты программного

¹ Приговор Кирсановского районного суда Тамбовской области по уголовному делу № 1-140/2019 от 28 августа 2019 г. // Сайт судебных и нормативных актов. URL: www.sudact.ru/regular/doc/NoCBWztR5OdC (дата обращения: 19.01.2024).

² Постановление Ангарского городского суда Иркутской области по уголовному делу № 1-1410/2019 от 29 ноября 2019 г. // Сайт судебных и нормативных актов. URL: www.sudact.ru/regular/doc/GLwzW3qei9rm (дата обращения: 19.01.2024).

обеспечения в ряде случаев имеют слабую устойчивость к хакерским атакам и не соответствуют требованиям по безопасности»¹.

Несомненно, одной из причин совершения киберпреступлений являются существующие пробелы в законодательстве, которые не позволяют быстро и эффективно привлечь к уголовной ответственности киберпреступников. Во-первых, по результатам проведенного нами опроса, 39,86% опрошенных граждан России и 38,44% граждан Казахстана считают, что несовершенство законодательства способствует совершению киберпреступлений. Во-вторых, 10,07% опрошенных сотрудников правоохранительных органов Российской Федерации и 38,27% Республики Казахстан считают, что конструктивные недостатки уголовно-правовых норм, устанавливающих ответственность за киберпреступления, затрудняют деятельность по выявлению, раскрытию и расследованию киберпреступлений.

«Преступник, пользуясь возможностью, „предоставленной государством“, ищет всевозможные лазейки ухода от ответственности, и пока правоохранительные органы и органы законодательной власти урегулируют вопрос восполнения пробела, нарушитель может скрыться. Профессионал своего дела, который заблаговременно готовил совершение киберпреступления, запросто может уйти от уголовной ответственности и вдобавок к этому совершить новые посягательства на информационную безопасность»².

Преступления, совершаемые с использованием ИТ-технологий, обусловлены целым комплексом факторов, относящихся к правовой, социально-экономической, политической, нравственно-психологической, технической и организационно-управленческой сферам. Следует признать, что долгое время данные факторы не принимались в учет при характеристике преступлений в сфере компьютерных технологий. Поэтому и сущность, и содержание данных преступлений понималось по-другому. Достаточно отметить тот факт, что при принятии

¹ Головинов О. Н., Погорелов А. В. Киберпреступность в современной экономике: состояние и тенденции развития // Вопросы инновационной экономики. 2016. № 6(1). С. 73–88.

² Диденко К. В. Некоторые проблемы выявления и предупреждения киберпреступлений // Вестник Белгородского юридического института МВД России. 2020. № 3. С. 20–24.

Уголовного кодекса Российской Федерации 1996 г. в нем была выделена самостоятельная глава 28 «Преступления в сфере компьютерной информации», в которой к компьютерным преступлениям были отнесены всего три состава преступлений: ст. 272 «Неправомерный доступ к компьютерной информации», ст. 273 «Создание, использование и распространение вредоносных программ для ЭВМ» и ст. 274 «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сетей». Лишь в последнее время данный перечень был расширен за счет еще двух статей: 274¹ и 274² УК РФ. Статья 274² «Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети „Интернет“ и сети связи общего пользования» была введена относительно недавно – 14 июля 2022 г.

В УК РФ не содержатся нормы, регулирующие уголовную ответственность за новые виды киберпреступлений. Отсутствуют федеральные и региональные программы, направленные на защиту жертв киберпреступлений, предупреждение преступлений в области компьютерной информации, а также пропаганду правовой и компьютерной грамотности среди населения¹.

В настоящее время существуют идеи о создании Инфокоммуникационного кодекса, который бы включал в себя положения нескольких существующих законов и воплощал новые современные разработки в информационной сфере в части контроля, регулирования и установления ответственности².

Одним из ключевых факторов, способствующих распространению киберпреступности среди населения, является недостаточное правовое воспитание, особенно в молодежной среде³. При воспитании молодых людей обычно акценти-

¹ Сидорова Е. З. О современных мерах предупреждения преступности // Современная наука. 2024. № 4. С. 48.

² Аккузин Ю. А., Леонов В. В. Кибернетические преступления как новая угроза обществу // Закон и право. 2020. № 4. С. 197–200.

³ Карабеков К. О. Некоторые вопросы профилактики киберпреступности в молодежной среде // Противодействие наркоугрозе на современном этапе: правовой и социально-гуманитарный аспекты : мат-лы междунар. науч.-практ. семинара. Красноярск, 2022. С. 97.

руется внимание на их правах, в то время как их обязанности, включая уважение к закону и окружающим, иногда не получают должного внимания¹.

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. Неправильное планирование и выделение ресурсов на кибербезопасность может вызывать ослабление защитных механизмов и увеличение вероятности успешных кибератак.

Одним из основных условий совершения подобных преступлений является отсутствие контроля со стороны руководства над действиями своих сотрудников и обслуживающего персонала. Это позволяет преступникам свободно использовать компьютерную технику, базы данных клиентов и другие технологические инструменты для совершения преступления, в том числе и с материальной выгодой.

Киберпреступники не всегда являются инициаторами преступлений в сфере компьютерных данных. Согласно результатам проведенного нами исследования в ряде случаев все начиналось с того, что к ним обращались третьи лица, которые предлагали специальные программные продукты для компьютеров и мобильных приложений, позволяющие незаконно получать доступ к мобильным телефонам граждан, особенно к мобильному банку, в целях кражи денежных средств. Более того, такие лица разъясняли приемы и способы совершения краж с использованием компьютерных и мобильных технологий и предлагали стать соучастниками преступления, совершить преступление в сфере компьютерных данных или с использованием мобильных технологий за определенное вознаграждение.

¹ Симонян К. Р. Правовое воздействие на личность: сущность и механизм реализации // Юридический вестник Кубанского государственного университета. 2023. № 4. С. 21–28.

Так, в Ростовской области в декабре 2018 г. работница салона связи гр. З. в социальной сети познакомилась с неустановленным лицом, предложившим ей заработок за предоставление ему информации об абонентах одного из сотовых операторов. Договорились о том, что неустановленное лицо будет ей присылать номера телефонов и паспортные данные абонентов, а гр. З. будет осуществлять неправомерный доступ к хранящейся на сервере компьютерной информации об указанных абонентах, а именно просматривать регистрационные данные абонентов и проверять баланс на счете, устанавливая количество контактов, после чего копировать полученную компьютерную информацию и передавать неустановленному лицу посредством сообщений в социальной сети. Параллельно З. занималась для неустановленного лица заменой телефонных номеров и перевыпуском sim-карт. За подобные деяния З. была осуждена по ч. 3 ст. 272 УК РФ и по пп. «а», «в» ч. 3 ст. 159⁶ УК РФ¹.

Еще одним из организационно-управленческих факторов, способствующих совершению киберпреступлений, является низкая раскрываемость данных преступлений. Следует отметить, что причин этого выделяется много.

На вопрос «Какие факторы, на Ваш взгляд, затрудняют деятельность по выявлению, раскрытию и расследованию киберпреступлений?» опрошенные нами сотрудники правоохранительных органов Российской Федерации (прил. 3) и Республики Казахстан (прил. 4), непосредственно принимавшие участие в раскрытии, расследовании или предупреждении киберпреступлений, дали ответы, которые приведены в табл. 4.

¹ Приговор Кировского районного суда г. Ростова-на-Дону Ростовской области по уголовному делу № 1-345/2019 от 13 сентября 2019 г. // Сайт судебных и нормативных актов. URL: www.sudact.ru/regular/doc/ (дата обращения: 19.01.2024).

Таблица 4 – Ответы сотрудников правоохранительных органов Российской Федерации (268 чел.) и Республики Казахстан (243 чел.) на вопрос «Какие факторы, на Ваш взгляд, затрудняют деятельность по раскрытию и расследованию киберпреступлений?», %

Факторы	Доля ответов сотрудников, %	
	РФ	РК
Отсутствие реальной возможности определения субъектов преступлений из-за недостаточной технической возможности	79,85	71,6
Сложности при производстве различного рода экспертиз, исследований	30,22	15,22
Чрезмерная сложность и запутанность уголовного законодательства	19,77	21,39
Отсутствие сложившейся судебной практики	19,77	13,16
Несовершенство уголовно-процессуального законодательства	19,77	–
Несовершенство законодательства об оперативно-розыскной деятельности	–	21,39
Сложности установления свидетельской базы	20,14	38,27
Конструктивные недостатки уголовно-правовых норм, устанавливающих ответственность за киберпреступления	10,07	38,27

В целом раскрытие, расследование и предупреждение киберпреступлений остается весьма трудной задачей для органов внутренних дел Российской Федерации и Республики Казахстан. Это, на наш взгляд, также объясняется трансграничным характером киберпреступлений, недостаточным системным анализом следственной и судебной практики, а также малой обеспеченностью практических работников методическими рекомендациями по организации расследования¹.

Внешние детерминанты связаны как с активными действиями недружественных государств по нарушению нормального развития наших государств, так и с отсутствием должного взаимодействия между государствами в борьбе с киберпреступностью, в связи с чем возникают условия для совершения киберпреступлений.

¹ Карабеков К. О. Проблемы предупреждения киберпреступлений в Республике Казахстан // Актуальные проблемы уголовной и уголовно-процессуальной политики Российской Федерации : мат-лы междунар. науч.-практ. конф. Омск : Сибирский юридический университет, 2023. С. 121.

В России и Казахстане существует угроза со стороны международных киберпреступных группировок и хакеров, которые могут использовать свои навыки и ресурсы для совершения киберпреступлений в данных странах. Эти группировки могут быть расположены в других странах и проводить свои атаки удаленно, что усложняет их обнаружение и преследование. По информации МВД РК, большинство интернет-мошенничеств, связанных с оформлением на граждан кредитов и займов, а также хищением их банковских накоплений, совершаются «зарубежными преступниками». Они входят в состав транснациональных организованных преступных групп, работающих по принципу Call-центров, с постоянной дислокацией в странах ближнего и дальнего зарубежья.

Использование вредоносного программного обеспечения и технологий из других стран: международные киберпреступные группировки и хакеры используют вредоносное программное обеспечение и технологии, разработанные в других странах, для осуществления своих атак. Это означает, что Россия и Казахстан сталкиваются с угрозами использования технологий, с которыми они незнакомы или для которых у них не хватает защитных мер.

Детерминантом киберпреступности также являются сложности, связанные с трудностями современной политической обстановки. Противостояние ряда европейских стран Российской Федерации в связи с возникшим конфликтом с Украиной оказал негативное влияние на экономическую сферу и затронул многие интересы государства и общества в целом. В сети Интернет идет информационная борьба, порождающая агрессию, используются все возможности причинения любого вреда как организациям, учреждениям и предприятиям России, так и отдельным ее гражданам. При этом ведется не только расистская и националистическая пропаганда в целях провокации гражданских конфликтов, но и мошенническое изъятие денежных средств у граждан.

Вследствие этих факторов обнаруживается сложность ведения малого и среднего бизнеса, особенно торговли импортными товарами, поскольку общение с иностранными партнерами ограничено, в связи с чем нередко происходит банкротство индивидуальных предпринимателей и физических лиц.

Подобные факторы вызывают рост безработицы, так как рабочие места сокращаются, а денежные потоки становятся менее интенсивными, что ведет к повышению стоимости товаров и услуг, а также провоцирует рост киберпреступности¹. Если, по данным Росстата, уровень безработицы в Российской Федерации сокращается и к концу 2024 г. составил 2,5%, а общая численность безработных достигла 1,9 млн человек², то в Республике Казахстан официальный уровень безработицы поднялся до 4,7%, а количество безработного населения насчитывало 449,8 тыс. человек³. Данные сведения важно учитывать при разработке мер предупреждения, потому что более 80% киберпреступлений совершается безработными местными жителями указанных стран.

Низкая заработная плата также является существенным фактором, который толкает киберпреступников к совершению преступлений. Поэтому многие из них готовы заниматься любым видом работы, даже связанным с преступной деятельностью, или же злоупотреблять своим служебным положением в целях получения материальной выгоды⁴.

Сложности в международном сотрудничестве в расследовании и раскрытии киберпреступлений: киберпреступления часто имеют международное измерение, что создает проблемы в международном сотрудничестве при расследовании и раскрытии этих преступлений. Различия в законодательстве, процедурах расследования и ограничении доступа к данным могут оказаться значительными преградами для эффективного сотрудничества между странами и обмена информацией.

Обобщая мнения ученых и судебную практику, предлагаем также обозначить внешние факторы киберпреступности, связанные не с самими киберпреступлениями, а именно с глобальной цифровизацией общества и государства.

¹ URL: https://kazpravda.kz/n/prichiny-vspleska-kiberprestupnosti-v-kazahstane-nazvali-v-mvd/?utm_source=yxnews&utm_medium=desktop&utm_referrer (дата обращения: 28.03.2025).

² URL: https://rosstat.gov.ru/labour_force/ (дата обращения: 28.03.2025).

³ URL: <https://stat.gov.kz/ru/industries/labor-and-income/stat-empt-unempl/> (дата обращения: 28.03.2025).

⁴ См., напр.: *Постановление* Балтасинского районного суда Республики Татарстан по уголовному делу № 1-45/2019 от 27 сентября 2019 г. // Сайт судебных и нормативных актов. URL: <https://sudact.ru/regular/doc/> (дата обращения: 13.01.2024).

По нашему мнению, эти факторы включают перенос значительной части повседневных функций, потребностей и интересов человека в виртуальную реальность, расширение области предоставления различных услуг с использованием информационных систем и технологий, увеличение разрыва между знаниями обычных пользователей компьютеров и скоростью развития информационно-коммуникационных ресурсов, доступность интернета для детей, которые начинают его использовать задолго до получения достаточных знаний о собственной безопасности, ограниченное вмешательство государственных органов и должностных лиц в функционирование информационно-коммуникационных технологий для обеспечения свободного доступа к информации, недостаточную компетентность правоохранительных органов в технических вопросах функционирования информационно-коммуникационных технологий¹.

Указанные факторы приводят к возникновению множества жертв киберпреступлений.

Стоит отметить, что эти факторы относятся главным образом к высококвалифицированным преступникам (хакерам). Но важно помнить о других категориях киберпреступников, которые, не являясь профессионалами, также совершают преступления. Для подобных преступников характерны другие факторы, такие как безработица и финансовые трудности, которые стимулируют их к использованию компьютерных технологий для совершения преступлений. Многие люди, оказавшиеся без работы и вынужденные выживать, соглашаются на предложения третьих лиц для совершения киберпреступлений, включая кражу личных данных или незаконную торговлю наркотиками через интернет.

Более того, приток новых цифровых технологий приводит к изменению динамики рынка труда, поскольку автоматизированные системы и искусственный интеллект вызывают технологическую безработицу, что играет значимую роль в возникновении и распространении киберпреступности.

¹ Жакупжанов А. О. Виктимологические факторы киберпреступности // Алтайский юридический вестник. 2019. № 3(27). С. 75–82.

В криминологических исследованиях можно найти описание и иных детерминант, которые способствуют наличию и распространению киберпреступности¹. Однако, на наш взгляд, наибольшую актуальность имеют выявление и анализ детерминант киберпреступлений в сравнительном аспекте специфики изучаемых нами стран, испытывающих негативное воздействие киберпреступности. Подобный подход позволяет найти решение проблемы поддержания правопорядка в информационном пространстве и среде на государственном уровне.

Исходя из анализа судебной практики, динамики, структуры и характера киберпреступности, учитывая мнения ученых, а также результаты опроса граждан, мы предлагаем выделять внутренние и внешние приоритетные детерминанты киберпреступности в России и Казахстане².

Среди внутренних детерминант, по нашему мнению, наиболее существенными являются:

1) 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;

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

¹ *Гришина Т. М.* Киберпреступность: глобальная угроза безопасности России и меры необходимого противодействия // Социально-экономические, этические и информационно-коммуникационные аспекты развития юриспруденции в эпоху цифровой революции : мат-лы науч.-практ. конф. / отв. ред. И. И. Грунтовский. М., 2019. С. 13–28 ; *Киданова Н. Л.* Актуальные проблемы современности – экономические преступления, совершаемые в киберпространстве // Вестник Белгородского юридического института МВД России им. И. Д. Путилина. 2018. № 1. С. 26–29 ; *Гомонов Н. Д.* Интернет: анализ криминогенных факторов // Научный портал МВД России. 2013. № 4(24). С. 34–38.

² *Карабеков К. О.* Детерминанты и меры предупреждения киберпреступлений в Российской Федерации и Республике Казахстан // Евразийский юридический журнал. 2025. № 7. С. 357.

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

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

4) 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.

Среди внешних детерминант, по нашему мнению, наиболее актуальными являются следующие:

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

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

Предложенная классификация выявленных детерминант киберпреступности в Российской Федерации и Республике Казахстан позволит оптимально выстраивать соответствующие меры по предупреждению киберпреступлений и защите физических и юридических лиц от киберпосягательств.

§ 2. Правовое обеспечение предупреждения киберпреступности

Предупреждение преступлений в самом широком смысле предполагает осуществление различных мер в экономической, политической, идеологической, культурной и бытовой сферах, направленных на искоренение или сдерживание неблагоприятных аспектов общественной жизни, которые могут выступать в качестве причин и условий для совершения преступлений. Такая организация общественной жизни должна быть обеспечена соответствующим правовым регулированием¹. Контроль общества над преступностью без надлежащей нормативной базы становится неэффективным². Особое значение такое правовое регулирование имеет в организации борьбы с киберпреступностью, поскольку в современное время наличие компетентной и тщательно проработанной уголовно-правовой политики в данной сфере является определяющим фактором борьбы с киберпреступностью. Как справедливо отмечают Е. М. Якимова и С. В. Нарутто, «правовое регулирование вопросов борьбы с киберпреступлениями представляет собой базис всей системы противодействия киберпреступности»³.

Учитывая рост киберпреступности, Российская Федерация и Республика Казахстан стремятся применять все возможные меры по ее предупреждению, однако при этом не всегда удается это делать только с помощью традиционных уголовно-правовых мер, тем более что сами способы совершения киберпреступлений очень быстро изменяются. Все это требует повышенного внимания к содержанию именно правового обеспечения деятельности по предупреждению киберпреступлений. Исходя из этого в настоящем исследовании правовое обеспечение предупреждения киберпреступлений рассматривается как один из важных видов обеспечения мер предупреждения киберпреступлений.

Под правовым обеспечением предупреждения киберпреступности следует понимать совокупность принимаемых государством законов и других норматив-

¹ *Криминология* : учебник / под ред. В. Д. Малкова. М., 2004. С. 140.

² *Шестаков Д. А.* Криминология: Преступность как свойство общества : краткий курс. СПб., 2001. С. 147–148.

³ *Якимова Е. М., Нарутто С. В.* Международное сотрудничество в борьбе с киберпреступностью // *Всероссийский криминологический журнал*. 2016. № 2. С. 372.

ных правовых актов, на основе которых принимаются организационные решения, регулирующие деятельность по предупреждению киберпреступности, осуществляется организация конкретных предупредительных мер обеспечения киберзащиты как государства и общества в целом, так и отдельного человека в частности.

Важность данных вопросов обусловлена тем, что недостаточное с точки зрения системности и своевременности законодательное регулирование всех вопросов, возникающих в сфере предупреждения киберпреступности, является одним из факторов, влияющих на рост киберпреступности в Российской Федерации и Республике Казахстан. Как отмечает ряд авторов, на сегодня нет достаточной нормативной правовой базы, позволяющей в полном объеме соблюсти законные права и свободы человека в интернет-пространстве¹. «В связи с этим необходимо совершенствовать отечественное законодательство по противодействию киберпреступности. Данную работу важно строить на основе изучения положительного зарубежного опыта по законодательному регулированию противодействия киберпреступности, не только внося изменения в действующие отечественные законодательные нормы, но и делая акценты на принятии новых законодательных норм, соответствующих современным реалиям»².

Законодательство о киберпреступности в России и Казахстане разнообразно, однако в целом не имеет комплексного характера, определенной системы, не представляет из себя единой системы. Осуществление деятельности по предупреждению киберпреступности без комплексной систематизированной нормативной базы в связи с хаотичностью, нехваткой государственной поддержки оказывается неэффективным. Для предупреждения киберпреступности в государстве необходимы, прежде всего, систематизированные, взаимосвязанные между собой нормативные правовые акты, охватывающие все вопросы организации и проведения деятельности по предупреждению киберпреступлений, в том числе и учитывающие вопросы международного взаимодействия. Тем более что международное сооб-

¹ *Кайгородова О. С.* Нормативно-правовое обеспечение кибербезопасности: защищены ли мы? // *Правопорядок: история, теория, практика.* 2023. № 4(39). С. 161.

² *Кобец П. Н.* Правовые основы предупреждения киберпреступлений: отечественный и зарубежный опыт // *Научный вестник Омской академии МВД России.* 2022. № 2(85). С. 105.

щество принимает активные меры по противодействию киберпреступности, однако достижение положительного результата возможно лишь при наличии единообразного подхода, использовании в национальном законодательстве схожих формулировок¹.

Примером действий в таком направлении могут служить действия наших государств. Так, стратегии Российской Федерации и Республики Казахстан по обеспечению кибербезопасности имеют схожие цели, представляя собой приоритетное направление обеспечения национальной безопасности государств, а также критически важных объектов. Обе страны обеспокоены безопасностью киберпространства, включая критическую информационную инфраструктуру. В рамках Содружества Независимых Государств обсуждаются вопросы сотрудничества в борьбе с киберпреступностью, подчеркиваются эволюция киберугроз, необходимость совместной работы и глобального регулирования действий в киберпространстве.

В целом законодательство Российской Федерации и Республики Казахстан о противодействии киберпреступности, как и других стран, в соответствии с международными нормами должны предусматривать решение следующих задач: 1) гарантировать защиту прав человека; 2) установить стандарты приемлемого поведения для пользователей информационно-коммуникационных технологий; 3) налагать социально-правовые санкции за киберпреступления; 4) защищать пользователей информационно-коммуникационных технологий в целом и смягчать или предотвращать вред, причиняемый им, системам, сервисам и инфраструктуре; 5) обеспечивать возможность проведения расследований и уголовного преследования в отношении преступлений, совершаемых в интернете (вне преде-

¹ *Преступления, совершаемые с использованием информационных технологий: проблемы квалификации и особенности расследования* : монография / А. Ф. Абдулвалиев, А. В. Белоусов, Ж. В. Вассалатий [и др.] ; под науч. ред. проф. Е. В. Смахтина, проф. Р. Д. Шарапова, доц. В. И. Морозова. Тюмень, 2021. С. 52 ; *Конев Д. А.* Криминологическая безопасность и ее обеспечение в сфере цифровых технологий : дис. ... канд. юрид. наук. Омск, 2022. С. 73.

лов реального мира); 6) содействовать международному сотрудничеству в вопросах, связанных с киберпреступлениями¹.

Оценивая современное состояние правового обеспечения кибербезопасности в Российской Федерации и Республике Казахстан, мы должны, прежде всего, определить содержание правовых основ предупреждения киберпреступлений в данных странах, поскольку в юридической литературе представлены несколько подходов к пониманию того, что должны охватывать правовые основы предупреждения киберпреступлений.

По мнению И. М. Мацкевича, нужно в целом учитывать то, что криминологическое законодательство представляет собой систему нормативных правовых актов, которые регулируют общественные отношения, связанные с причинами, условиями, предупреждением и борьбой с преступлениями и преступностью, а также с применением соответствующих мер². Согласно позиции А. Л. Осипенко, вопросы правового регулирования предупреждения киберпреступлений охватывают два направления: 1) развитие общих правовых механизмов для обеспечения безопасности информационного пространства глобальных компьютерных сетей; 2) создание системы правовых норм, которые непосредственно регулируют борьбу с преступностью в глобальных сетях³.

В. Ф. Джафарли предлагает систематизировать нормативные правовые акты по обеспечению кибербезопасности в Российской Федерации согласно трем уровням: первый – правовые основы обеспечения национальной безопасности, второй – правовые основы обеспечения национальной и международной кибербезопасности, третий – правовые основы обеспечения криминологической безопасности, включая сферу информационно-коммуникационных технологий⁴.

¹ *Киберпреступность*. Модуль 3. Правовая база и права человека // ООН. Вена, 2019. С. 4. [Cybercrime_Module_3_Legal_Frameworks_and_Human_Rights_RU.pdf](#) (дата обращения: 13.01.2023).

² *Мацкевич И. М.* Криминология : учебник для аспирантов. М., 2017. С. 13–14.

³ *Осипенко А. Л.* Сетевая компьютерная преступность: теория и практика борьбы : монография. Омск, 2009. С. 314.

⁴ *Джафарли В. Ф.* Криминология кибербезопасности : в 5 т. Т. 1 : Криминологическая кибербезопасность: теоретические, правовые и технологические основы. М., 2021. С. 20.

Для лучшего отражения содержания системы нормативных правовых актов, выявления пробелов и дублирования в правовом регулировании вопросов кибербезопасности и предупреждения киберпреступности в Российской Федерации и Республике Казахстан мы предлагаем проводить классификацию нормативных правовых актов по субъектам, принимающим нормативные правовые акты.

Мы считаем, 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)¹.

Учитывая трансграничный (транснациональный) характер киберпреступлений, при котором преступник, объект преступного посягательства, жертва могут находиться под юрисдикцией разных государств, к первой группе следует относить международно-правовые акты Организации Объединенных Наций (ООН) по обеспечению кибербезопасности (информационной безопасности) и сотрудничеству по борьбе с киберпреступностью.

К таким источникам относятся документы ООН, посвященные вопросам международной информационной безопасности. Рассмотрим их.

1. Резолюция Генеральной Ассамблеи ООН 73/27 от 5 декабря 2018 г. «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности»². Данная резолюция базируется на богатом позитивном опыте работы Группы правительственных экспертов ООН по международной информационной безопасности. Группе созыва 2014–2015 гг. удалось достичь кон-

¹ Карабеков К. О. Правовое обеспечение предупреждения киберпреступности в Российской Федерации и Республике Казахстан // Известия Юго-Западного государственного университета. Серия «История и право». 2023. Т. 13, № 3. С. 160–161.

² Официальный сайт ООН. URL: <https://www.un.org/disarmament/ru/> (дата обращения: 13.01.2023).

сенсуса по целому ряду принципиальных вопросов, связанных с использованием информационно-коммуникационных технологий, в частности, по поводу того, что: 1) эти технологии должны использоваться исключительно в мирных целях, а международное сотрудничество необходимо направить на предотвращение конфликтов в информационном пространстве; 2) в цифровой сфере действуют такие общепризнанные международно-правовые принципы, как неприменение силы или угрозы силой, уважение суверенитета, невмешательство во внутренние дела государств; 3) государства обладают суверенитетом над информационно-коммуникационной инфраструктурой на своей территории; 4) любые обвинения в адрес государств в причастности к кибератакам должны быть подкреплены доказательствами; 5) государства не должны использовать посредников для осуществления кибератак и не допускать того, чтобы их территории использовались в этих целях; 6) государства должны бороться с использованием скрытых вредоносных функций – так называемых «закладок» – в ИТ-продукции¹.

2. Резолюция Генеральной Ассамблеи ООН 73/264 от 22 декабря 2018 г. «Поощрение ответственного поведения государств в киберпространстве в контексте международной безопасности»². Этот документ направлен на формирование международных норм и правил в киберпространстве, которые предполагают ответственное поведение государств в данной сфере. Он призывает государства следовать международным нормам и принципам в киберпространстве, включая уважение человеческих прав и основных свобод, предотвращение применения кибертехнологий в военных целях, защиту критической информационной инфраструктуры и предупреждение киберпреступности. Он является важным инструментом для повышения безопасности в киберпространстве и предотвращения различных видов киберугроз, таких как кибератаки, кибершпионаж и кибертерроризм. Последствия киберпреступности могут быть разрушительными и затрагивать как государственные, так и частные секторы общества, поэтому резолюция играет важную роль в укреплении международной безопасности, содействует сотрудни-

¹ URL: https://www.mid.ru/ru/foreign_policy/news/1518395/ (дата обращения: 12.05.2024).

² Там же.

честву между государствами и создает основу для разработки эффективных стратегий в области кибербезопасности. Ее реализация способствует укреплению глобальной стабильности и содействует устойчивому развитию мирового информационного пространства.

3. Резолюцией 79/243 Генеральной Ассамблеи от 24 декабря 2024 г. принята единая международная «Конвенция Организации Объединенных Наций против киберпреступности; укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям»¹. Данную конвенцию следует отметить особо уже в связи с тем, что в ней в качестве основной цели выделяется необходимость предупреждения киберпреступности. Так, в Конвенции в качестве целей выделяются: а) содействие принятию и укреплению мер, направленных на повышение эффективности и результативности предупреждения киберпреступности и борьбы с ней; б) поощрение, облегчение и укрепление международного сотрудничества в предупреждении киберпреступности и борьбе с ней; и с) поощрение, облегчение и поддержка технической помощи и создания потенциала в целях предупреждения киберпреступности и борьбы с ней, особенно в интересах развивающихся стран.

Данная конвенция открыта для подписания в Ханое в 2025 г., а затем в Центральных учреждениях Организации Объединенных Наций в Нью-Йорке до 31 декабря 2026 г. Нашим странам необходимо подписать и ратифицировать ее в установленные сроки.

4. Конвенция ООН против транснациональной организованной преступности 2000 г.², устанавливающая стандарты и подходы к борьбе с преступностью, описывающая методы сотрудничества между государствами в борьбе с организованной

¹ Официальный сайт ООН. URL: <https://www.un.org/ru/documents/treaty/A-RES-79-243> (дата обращения: 12.04.2025).

² Конвенция ООН против транснациональной организованной преступности : принята в Нью-Йорке 15 ноября 2000 г. // Собрание законодательства Российской Федерации. 2004. № 40, ст. 3882.

преступностью, включая киберпреступность. Конвенция обязывает государства принимать меры для предотвращения, расследования преступлений, связанных с использованием информационно-коммуникационных технологий, и наказания за них. Она также предусматривает сотрудничество и обмен информацией между государствами для эффективного пресечения киберпреступности.

5. Факультативный протокол к Конвенции ООН о правах ребенка, касающийся торговли детьми, детской проституции и детской порнографии, принятый 25 мая 2000 г.¹, имеющий целью сохранить права детей на защиту от торговли, проституции и порнографии. В современном мире с развитием интернета и цифровых технологий дети становятся все более уязвимыми перед угрозами киберпреступности, и данный протокол играет важную роль в борьбе с киберпреступностью и защите прав детей от угроз в онлайн-среде.

6. Элементы для создания глобальной культуры кибербезопасности, принятые Резолюцией 57/239 Генеральной Ассамблеи ООН от 20 декабря 2002 г.² и содержащие ключевые элементы для создания глобальной культуры кибербезопасности, представляющие собой набор принципов, рекомендаций и мер, которые способствуют укреплению безопасности в киберпространстве. Элементы этой стратегии включают в себя сотрудничество между государствами, международное партнерство, защиту прав человека и основных свобод в киберпространстве, а также обеспечение безопасности критической информационной инфраструктуры. Кроме того, документ призывает к принятию мер по борьбе с киберпреступностью, в том числе путем совершенствования законодательства и укрепления международного сотрудничества.

В ООН есть несколько документов, в том числе глобальная программа кибербезопасности Международного союза электросвязи и Резолюция Генеральной Ассамблеи о создании глобальной культуры кибербезопасности и оценке нацио-

¹ *Официальный сайт ООН.* URL: <https://www.un.org/disarmament/ru/> (дата обращения: 13.01.2023).

² *Официальный сайт ООН.* URL: https://www.un.org/ru/documents/decl_conv/conventions/ (дата обращения: 13.01.2023).

нальных усилий по защите важнейших информационных инфраструктур¹. В этих документах приводятся подходы к пониманию кибербезопасности, включая безопасное использование информационно-коммуникационных технологий в целях обеспечения неприкосновенности частной жизни, конфиденциальности, целостности и доступности информации в электронной форме, а также защиты критической информационно-коммуникационной инфраструктуры, взаимодействующей с интернетом. Эта инфраструктура включает информационные системы, аппаратно-программные комплексы, телекоммуникационные системы, сети связи, системы защиты информации и программного обеспечения от вредоносных программно-технических воздействий.

Однако в данных документах не нашли отражение многие важные для противодействия киберпреступности понятия. Так, термин «кибербезопасность» и все его производные (киберпространство, киберзащита, кибератаки, кибернападение, киберпреступность и др.) не имеют единого, общепринятого юридического определения. ООН как глобальная организация коллективной безопасности должна предложить государствам адекватные правовые и политические инструменты для обеспечения приемлемого уровня кибербезопасности (информационной безопасности). Поэтому неслучайно, что теория уголовного права до настоящего времени не располагает единым пониманием киберпреступности как предмета преступного посягательства. В том числе в недостаточной мере учтены проблемы развития терминологии в сфере киберпреступности, есть множественные пробелы в уголовном законодательстве по вопросам, регулирующим уголовную ответственность за совершение новейших киберпреступлений².

В качестве первоочередных мер необходимо разработать **единый подход к определению киберпреступности** и закрепить в нормативных актах определения таких понятий, как «интернет», «киберпреступление», «киберпреступность», «киберпространство». Отсутствие этих дефиниций позволяет преступникам избе-

¹ URL: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N09/474/51/PDF/N0947451.pdf?Open-Element> (дата обращения: 13.01.2024).

² Кобец П. Н. Указ. соч. С. 102.

гать ответственности, пользуясь различиями в правовых основах разных государств.

К международно-правовым актам межнационального уровня следует отнести акты таких организаций, как Совет Европы (СЕ) (47 государств), Организация по безопасности и сотрудничеству в Европе (ОБСЕ) (57 государств), Шанхайская организация сотрудничества (ШОС) (9 государств), Содружество Независимых Государств (СНГ) (10 государств)¹.

К международно-правовым актам межнационального уровня, посвященным вопросам международной информационной безопасности (кибербезопасности) и борьбы с киберпреступностью относятся:

– на уровне СЕ: Конвенция Совета Европы о компьютерных преступлениях и Дополнительный протокол к Конвенции о компьютерных преступлениях, касающийся уголовной ответственности за акты расистского и ксенофобского характера, совершаемые через компьютерные системы 2001 г.², Конвенция Совета Европы о защите детей от эксплуатации и надругательств сексуального характера 2007 г.³;

– на уровне ОБСЕ: Меры укрепления доверия в рамках Организации по безопасности и сотрудничеству в Европе (ОБСЕ) с целью сокращения рисков возникновения конфликтов в результате использования информационных и коммуникационных технологий, Решение PC.DEC/1202 от 10 марта 2016 г.⁴;

¹ *Карабеков К. О.* Правовое обеспечение предупреждения кибербезопасности в Российской Федерации и Республике Казахстан. С. 161–162.

² *Конвенция* о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23 ноября 2001 г.) : с изменениями от 28 января 2003 г. Доступ из справ.-правовой системы «Гарант».

³ *О ратификации* Конвенции Совета Европы о защите детей от сексуальной эксплуатации и сексуальных злоупотреблений: федеральный закон от 7 мая 2013 г. № 76-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

⁴ *Меры* укрепления доверия в рамках ОБСЕ с целью сокращения рисков возникновения конфликтов в результате использования информационных и коммуникационных технологий : решение No PC.DEC/1202 ОБСЕ от 10 марта 2016 г. // Официальный сайт ОБСЕ. URL: <https://www.osce.org/ru/pc/228521?download=true> (дата обращения: 25.02.2024).

– на уровне ШОС: Соглашение между правительствами государств – членов Шанхайской организации сотрудничества (ШОС) о сотрудничестве в области обеспечения международной информационной безопасности 2010 г.¹;

– на уровне СНГ: Соглашение о сотрудничестве в борьбе с преступлениями в сфере компьютерной информации от 1 июня 2001 г.²; Модельный информационный кодекс для государств – участников СНГ от 23 ноября 2012 г.³; Рекомендации Межпарламентской ассамблеи государств СНГ по совершенствованию и гармонизации национального законодательства государств – участников СНГ в сфере обеспечения информационной безопасности от 23 ноября 2012 г.⁴; Рекомендации Межпарламентской ассамблеи государств СНГ по правовому регулированию эксплуатации открытых телекоммуникационных сетей для предупреждения их использования в террористических и иных противоправных целях от 29 ноября 2013 г.⁵; Модельный закон СНГ о критически важных объектах информационно-коммуникационной инфраструктуры от 28 ноября 2014 г.⁶; Модельный Регламент административных процедур, осуществляемых уполномоченными органами в сфере обеспечения информационной безопасности государств – участников

¹ *Об утверждении* Соглашения между правительствами государств – членов Шанхайской организации о сотрудничестве в области обеспечения международной информационной безопасности : распоряжение Правительства Российской Федерации от 16 июля 2009 г. № 984-р // Собрание законодательства Российской Федерации. 2009. № 30, ст. 3879.

² *Соглашение* о сотрудничестве государств – участников Содружества Независимых Государств с преступлениями в сфере компьютерной информации (Минск, 1 июня 2001 г.) // Собрание законодательства Российской Федерации. 2009. № 13, ст. 1460.

³ *Модельный* информационный кодекс для государств – участников Содружества Независимых Государств : принят в г. Санкт-Петербурге 23 ноября 2012 г. постановлением № 38-6 на 38-м пленарном заседании Межпарламентской Ассамблеи государств – участников Содружества Независимых Государств // Информационный бюллетень Межпарламентской Ассамблеи государств – участников Содружества Независимых Государств. 2013. № 57, ч. 1.

⁴ *Постановление* Межпарламентской Ассамблеи государств – участников Содружества Независимых Государств от 23 ноября 2012 г. № 38-20 // Там же.

⁵ *Рекомендации* по правовому регулированию эксплуатации открытых телекоммуникационных сетей для предупреждения их использования в террористических и иных противоправных целях : постановление № 39-25 Межпарламентской Ассамблеи государств – участников Содружества Независимых Государств : принято в г. Санкт-Петербурге от 29 ноября 2013 г. // Там же. № 57, ч. 2.

⁶ *О модельном* законе «О критически важных объектах информационно-коммуникационной инфраструктуры» : постановление № 41-14 Межпарламентской Ассамблеи государств – участников Содружества Независимых Государств : принято в г. Санкт-Петербурге 28 ноября 2014 г. // Там же. 2015. № 62, ч. 2.

СНГ от 28 ноября 2014 г.¹; Рекомендации Межпарламентской ассамблеи государств СНГ по совершенствованию законодательства государств – участников СНГ в сфере противодействия технологическому терроризму от 16 апреля 2015 г.²

Несомненно, все указанные документы являются фундаментальными актами при решении вопросов по борьбе с киберпреступностью на международном уровне. Однако Россия не присоединилась к Конвенции Совета Европы о компьютерных преступлениях и дополнительному протоколу к ней, касающемуся уголовной ответственности за акты расистского и ксенофобского характера, совершаемые через компьютерные системы 2001 г. Это связано с тем, что положения статьи 32b противоречат российскому законодательству и нарушают суверенитет государства, так как предусмотренные в ней действия могут осуществляться без предварительного уведомления и согласия стороны, на территории которой эти действия совершаются. Кроме того, в Уголовном кодексе Российской Федерации отсутствуют нормы, устанавливающие уголовную ответственность юридических лиц за преступления в сфере компьютерной информации³.

К нормативным правовым актам **национального законодательства**, обеспечивающим кибербезопасность (информационную безопасность) стран, следует отнести законы и подзаконные нормативные правовые акты.

Безусловно, главным правовым источником защиты прав граждан и обеспечения кибербезопасности является Конституция. Согласно ст. 23 Конституции Российской Федерации каждый имеет право на неприкосновенность част-

¹ *О модельном Регламенте административных процедур, осуществляемых уполномоченными органами в сфере обеспечения информационной безопасности государств – участников Содружества Независимых Государств* : постановление № 41-17 Межпарламентской Ассамблеи – участников Содружества Независимых Государств : принято в г. Санкт-Петербурге 28 ноября 2014 г. // Там же.

² *О Рекомендациях по совершенствованию законодательства о выборах глав государств в странах Содружества Независимых Государств* : постановление № 40-12 Межпарламентской Ассамблеи государств – участников Содружества Независимых Государств : принято в г. Санкт-Петербурге 18 апреля 2014 г. // Там же. 2014. № 61.

³ *Евдокимов К. Н.* Актуальные вопросы предупреждения киберпреступности в Российской Федерации // Актуальные проблемы борьбы с преступностью: вопросы теории и практики : мат-лы XV междунар. науч.-практ. конф. : в 2 ч. Красноярск, 2022. Ч. 2. С. 58–59.

ной жизни, личную и семейную тайну, защиту своей чести и доброго имени (п. 1), а также каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (п. 2). Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются (п. 1 ст. 24)¹. Аналогичные статьи имеются и в Конституции Республики Казахстан (ст. ст. 17–18)². Это говорит о том, что государства также гарантируют защиту личных неимущественных прав граждан от противоправных посягательств с использованием информационно-коммуникационных технологий.

К основным нормативным правовым актам, обеспечивающим кибербезопасность (информационную безопасность) стран, следует отнести Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»³ и приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 30 июня 2023 г. № 221/НК «Об утверждении Правил и критериев отнесения объектов информационно-коммуникационной инфраструктуры к критически важным объектам информационно-коммуникационной инфраструктуры»⁴. Оба нормативных правовых акта являются важными для предупреждения киберпреступности в России и Казахстане, в их положениях обращается внимание на критически важные объекты информационно-коммуникационной инфраструктуры и предлагаются конструктивные меры для их защиты. Федеральный закон Российской Федерации нацелен на безопасность критической информационной инфраструктуры, устанавливает юридическую базу для предупреждения киберпреступности, задает рамки ответственности и меры защиты данных критически важных объектов. Указанный федеральный закон предоставляет органам государственной власти

¹ Конституция Российской Федерации : принята всенародным голосованием 12 декабря 1993 г., с изм., одобренными в ходе общероссийского голосования 1 июля 2020 г. // Российская газета. 1993. 25 дек. ; 2020. 4 июля.

² Конституция Республики Казахстан : принята на республиканском референдуме 30 августа 1995 г. // Казахстанская правда. 1995. 5 сент.

³ О безопасности критической информационной инфраструктуры Российской Федерации : федеральный закон от 26 июля 2017 г. № 187-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

⁴ URL: <https://adilet.zan.kz/rus/docs/V2300032996> (дата обращения: 15.02.2024).

правовые инструменты для пресечения и предотвращения угроз кибербезопасности. Он также обязывает критические объекты информационно-коммуникационной инфраструктуры осуществлять аудит систем безопасности и устанавливать соответствующие меры для защиты сетей и данных от кибератак.

Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 30 июня 2023 г. № 221/НК, в свою очередь, определяет критерии и правила, по которым объекты информационно-коммуникационной инфраструктуры могут быть отнесены к критически важным. Документ создает основу для объективной классификации и оценки уровня кибербезопасности объектов информационно-коммуникационной инфраструктуры. Правила отнесения к критически важным объектам информационно-коммуникационной инфраструктуры прописывают процедуру утверждения критериев отнесения объектов к категории критически важных и обязывают их владельцев обеспечить высокий уровень защиты от киберугроз.

В контексте предупреждения киберпреступности в России и Казахстане Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации»¹ и Закон Республики Казахстан от 16 ноября 2015 г. № 401-V ЗРК «О доступе к информации»² играют важную роль в защите информации и информационных технологий.

Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации» предоставляет обширный круг правил и норм, регулирующих использование информационных технологий и обеспечение безопасности информации. Он предусматривает механизмы для защиты критической информации в различных сферах, включая государственные органы и организации, а также провайдеров интернет-услуг. Закон помогает предупредить киберпреступность через установление требований к хранению, передаче, обработке и защите информации.

¹ *Об информации, информационных технологиях и защите информации* : федеральный закон от 27 июля 2006 г. № 149-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

² *О доступе к информации* : Закон Республики Казахстан от 16 ноября 2015 г. № 401-V ЗРК // Казахстанская правда. 2015. 19 нояб.

Закон Республики Казахстан от 16 ноября 2015 г. № 401-V ЗРК «О доступе к информации» также играет важную роль в предупреждении киберпреступности. Он обеспечивает основы для регулирования доступа к информации в Казахстане и определяет процедуры, обязанности и права государственных органов, поставщиков информации и общественности. Закон способствует прозрачности и открытости информационных процессов, что является важным элементом в снижении возможностей киберпреступников.

Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»¹ и Закон Республики Казахстан от 21 мая 2013 г. «О персональных данных и их защите»² устанавливают основные правила использования персональных данных, включая их сбор, обработку и хранение. В законах предусмотрены наказания для нарушителей, что создает стимул соблюдать законодательство и предупреждает возможные киберпреступления, связанные с утечкой персональных данных.

Закон Республики Казахстан устанавливает правила пользования персональными данными и предоставляет гражданам контроль над своими данными, определяет ответственность организаций в случае нарушения закона. Кроме того, важное значение придается праву на «забвение» – возможности удалить свои персональные данные из баз данных. Закон направлен на защиту граждан от киберпреступлений, связанных с незаконной обработкой персональных данных и утечкой конфиденциальной информации.

Оба акта нацелены на защиту персональных данных граждан и предупреждение киберпреступности. Однако следует отметить, что они имеют некоторые различия в подходе и деталях применения. В России этот закон принят раньше, и в последние годы более активно принимаются меры для усиления контроля за передачей и обработкой персональных данных.

¹ *О персональных данных* : федеральный закон от 27 июля 2006 г. № 152-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

² *О персональных данных и их защите* : Закон Республики Казахстан от 21 мая 2013 г. // Казахстанская правда. 2013. 25 мая.

Доктрина информационной безопасности Российской Федерации¹ и постановление Правительства Республики Казахстан от 30 июня 2017 г. № 407 «Об утверждении Концепции кибербезопасности»² позволяют понять основные принципы и подходы, осуществляемые в данной области. Эти документы, разработанные с учетом современных вызовов и угроз, определяют стратегические цели и задачи в сфере информационной безопасности, а также механизмы и инструменты для их достижения.

Важным элементом в предупреждении киберпреступности является **сотрудничество** между государствами³. Постановление Правительства Республики Казахстан от 30 июня 2017 г. № 407 «Об утверждении Концепции кибербезопасности» свидетельствует о стремлении казахстанского правительства активно принимать участие в международных усилиях по предотвращению киберугроз и кибератак. Концепция кибербезопасности определяет основные принципы, цели и задачи в данной области, а также обозначает инструменты и механизмы для защиты информационных систем страны.

Немаловажно отметить, что нормативные правовые акты, регулирующие предупреждение киберпреступности, должны обеспечивать баланс между защитой информационных систем и соблюдением прав и свобод граждан. В рамках доктрины информационной безопасности Российской Федерации и концепции кибербезопасности Республики Казахстан заложены механизмы, ориентированные на установление правил использования информации, защиту персональных данных и недопущение несанкционированного доступа к информации, а также применение мер противодействия киберпреступности. В целом, как отмечает А. Л. Осипенко, эффективная борьба с преступностью в интернете становится возможной только при принятии комплексных нормативных правовых актов, ко-

¹ Об утверждении Доктрины информационной безопасности Российской Федерации : Указ Президента РФ от 5 ноября 2016 г. №. Доступ из справ.-правовой системы «Консультант-Плюс».

² Об утверждении Концепции кибербезопасности : постановление Правительства Республики Казахстан от 30 июня 2017 г. № 407. URL: <https://adilet.zan.kz/rus/docs/P1700000407> (дата обращения: 11.02.2024).

³ Лопатина Т. М. Криминологические и уголовно-правовые основы противодействия компьютерной преступности : дис. ... д-ра юрид. наук. М., 2006. С. 21–22.

торые учитывали бы реальную криминогенную обстановку в сфере сетевого информационного пространства¹.

Стратегия развития информационного общества в Российской Федерации на 2017–2030 гг.², национальная программа «Цифровая экономика Российской Федерации»³ и постановление Правительства Республики Казахстан от 30 декабря 2021 г. № 961 «Об утверждении Концепции развития отрасли информационно-коммуникационных технологий и цифровой сферы»⁴ являются ключевыми документами в цифровой сфере развития информационного общества. Они устанавливают основные направления и приоритеты развития цифровой экономики, в том числе и меры по борьбе с киберпреступностью.

В рамках **национальной программы** «Цифровая экономика Российской Федерации» также уделяется особое внимание вопросам кибербезопасности. Программа охватывает широкий спектр мер и проектов, направленных на защиту информационных ресурсов и предотвращение кибератак. Отраслевые программы, созданные в рамках национальной программы, дополняют и уточняют нормативно-правовую базу, регламентирующую противодействие киберпреступности.

Нельзя не упомянуть и постановление Правительства Республики Казахстан от 30 декабря 2021 г. № 961 «Об утверждении Концепции развития отрасли информационно-коммуникационных технологий и цифровой сферы». Оно ставит приоритетные задачи по развитию цифровой экономики в стране и уделяет особое внимание вопросам кибербезопасности и противодействию киберпреступности. Постановление определяет планы и направления работы в данной области и предлагает меры по укреплению киберзащиты, адаптации к новым технологическим

¹ *Осипенко А. Л.* Указ. соч. С. 312.

² *Стратегия* развития информационного общества в Российской Федерации на 2017–2030 гг. Доступ из справ.-правовой системы «КонсультантПлюс».

³ *Об утверждении* программы «Цифровая экономика Российской Федерации» : распоряжение Правительства Российской Федерации от 28 июля 2017 г. № 1632-р. Доступ из справ.-правовой системы «КонсультантПлюс».

⁴ *Об утверждении* Концепции развития отрасли информационно-коммуникационных технологий и цифровой сферы : постановление Правительства Республики Казахстан от 30 декабря 2021 г. № 961. URL: <https://adilet.zan.kz> (дата обращения: 13.01.2024).

вызовам и совершенствованию правовой базы, регулирующей деятельность в сфере информационных технологий.

Национальная стратегия развития искусственного интеллекта на период до 2030 г., утвержденная Указом Президента Российской Федерации от 10 октября 2019 г. № 490¹, представляет собой пример стратегического подхода к предупреждению преступлений в сфере информационной безопасности и стимулирует развитие и использование технологий искусственного интеллекта для достижения этой цели. Один из основных аспектов данного нормативного правового акта – обеспечение создания и развития систем искусственного интеллекта, которые будут способствовать эффективному обнаружению, предупреждению и расследованию киберпреступлений. Важно отметить, что здесь учитываются не только технические аспекты, но и этические и правовые нормы, которые должны сопровождать деятельность таких систем.

Нормативный правовой акт также создает основу для сотрудничества между различными государственными организациями, образовательными учреждениями и частным сектором. Это сотрудничество имеет стратегическое значение для обмена информацией, разработки общих стандартов и единых подходов в развитии искусственного интеллекта.

Одним из ключевых направлений этой национальной стратегии является создание гарантий и защит для лиц, пользующихся системами искусственного интеллекта. Разработка соответствующих норм и правил обеспечит сохранность конфиденциальности, целостности и доступности информации, а также эффективную защиту от попыток незаконного доступа к данным и несанкционированного их использования.

Этот нормативный правовой акт направлен на создание устойчивой и конкурентоспособной экосистемы искусственного интеллекта, которая будет способствовать предупреждению киберпреступности, включая различные формы

¹ *О развитии* искусственного интеллекта в Российской Федерации (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года») : Указ Президента Российской Федерации от 10 ноября 2019 г. № 490. Доступ из справ.-правовой системы «КонсультантПлюс».

мошенничества, внедрение вредоносного программного обеспечения и другие виды информационных атак. Такой подход является ключевым фактором в обеспечении безопасности информационного пространства и успеха страны в цифровой эпохе.

Для эффективного и системного правового регулирования кибербезопасности требуется определенная стратегия. В связи с этим постановлением Правительства Республики Казахстан от 30 июня 2017 г. № 407 была утверждена **Концепция** кибербезопасности¹. Данная концепция определяет основные направления реализации государственной политики в области защиты информационных ресурсов, информационных систем и телекоммуникационных сетей, а также обеспечения безопасного использования информационно-коммуникационных технологий. Кроме того, она направлена на единство подходов к контролю обеспечения информационной безопасности государственных органов, физических и юридических лиц, а также на разработку механизмов предупреждения и оперативного реагирования на инциденты информационной безопасности, включая случаи чрезвычайных ситуаций различного характера, а также в условиях введения чрезвычайного или военного положения.

Формально подобная концепция кибербезопасности в Российской Федерации отсутствует, хотя в 2010 г. был опубликован проект похожей концепции, но в итоге такой документ не был принят. В качестве аналогов стратегии кибербезопасности в Российской Федерации можно привести такие нормативные правовые акты, как Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации, утвержденные Президентом Российской Федерации 3 февраля 2013 г. № 803², и Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Феде-

¹ *Об утверждении* Концепции кибербезопасности («Киберцит Казахстана») : постановление Правительства Республики Казахстан от 30 июня 2017 г. № 407. URL: <https://adilet.zan.kz/rus/docs/> (дата обращения: 13.01.2024).

² URL: <http://www.scrf.gov.ru> (дата обращения: 14.02.2023).

рации», а также Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации¹, выписка из которой опубликована на сайте Совета безопасности. Учитывая опыт Республики Казахстан по актуализации государственной политики в области кибербезопасности, считаем необходимым принятие Концепции кибербезопасности в Российской Федерации².

В настоящее время в Российской Федерации и Республике Казахстан сформирована определенная правовая основа, направленная на предупреждение киберпреступности. Важное значение для правового обеспечения предупреждения киберпреступлений имеют уголовно-правовые меры противодействия киберпреступности. Как показало проведенное исследование, в современных условиях большую актуальность для наших стран имеют вопросы совершенствования уголовно-правовой основы борьбы со всеми разновидностями киберпреступности.

В Уголовном кодексе Российской Федерации нормы о преступлениях, совершаемых в сфере информационных технологий, выделены в самостоятельную главу 28 «Преступления в сфере компьютерной информации»: ст. 272 (Неправомерный доступ к компьютерной информации); ст. 273 (Создание, использование и распространение вредоносных компьютерных программ); ст. 274 (Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей); ст. 274¹ (Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации); ст. 274² (Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования).

¹ *Выписка* из Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, утвержденной Президентом Российской Федерации 12 декабря 2014 г. № К 1274. URL: <http://www.fsb.ru/> (дата обращения: 14.02.2023).

² *Карабеков К. О.* Правовое обеспечение предупреждения киберпреступности в Российской Федерации и Республике Казахстан. С. 164.

Кроме того, Федеральным законом от 8 августа 2024 г. № 218-ФЗ введен пункт «т» ч. 1 ст. 63 УК РФ (совершение умышленного преступления с публичной демонстрацией, в том числе в средствах массовой информации или информационно-телекоммуникационных сетях (включая сеть «Интернет»).

Пункт «т» ч. 1 ст. 63 УК РФ устанавливает ответственность за совершение умышленного преступления с публичной демонстрацией его результатов. Это включает в себя действия, которые осуществляются через средства массовой информации или информационно-телекоммуникационные сети, в том числе сеть «Интернет». Данная норма подчеркивает важность общественной безопасности и моральных норм, а также стремление законодателя предотвратить распространение информации, способствующей совершению преступлений или оправдывающей их. Таким образом, закон направлен на защиту общества от негативного влияния, которое может оказывать публичное освещение преступной деятельности.

Национальное законодательство Республики Казахстан также предусматривает уголовную ответственность за совершение преступлений с использованием информационных технологий. В последние годы Казахстан принял ряд законодательных мер, целью которых является борьба с киберпреступлениями. В настоящее время в действующем Уголовном кодексе Республики Казахстан¹ соответствующие уголовные правонарушения предусмотрены в отдельной главе. Кроме того, квалифицирующие признаки, связанные с использованием информационных технологий и сетей коммуникаций, включены в статьи, расположенные в других разделах УК РК. В Уголовном кодексе старой редакции (от 16 июля 1997 г.) все преступления в сфере информационных технологий были сгруппированы в ст. 227 УК РК «Неправомерный доступ к компьютерной информации, создание, использование и распространение вредоносных программ для ЭВМ», которая

¹ Уголовный кодекс Республики Казахстан от 3 июля 2014 г. № 226-V ЗПК. URL: <https://adilet.zan.kz/rus/docs/K1400000226> (дата обращения: 01.02.2025).

предусматривала ответственность за неправомерный доступ к охраняемой законом компьютерной информации¹.

Отдельного внимания заслуживают постановление Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть „Интернет“»², которое разъясняет и обеспечивает единообразное применение судами Российской Федерации законодательства об уголовной ответственности за преступления в сфере компьютерной информации, предусмотренные ст. ст. 272, 273, 274 и 274¹ УК РФ, а также за иные преступления, совершенные с использованием электронных или информационно-телекоммуникационных сетей, включая сеть Интернет.

В России осмысление феномена киберпреступности как неизвестной ранее формы уголовно наказуемых деяний началось с положений Уголовного кодекса 1996 г. С этого времени не было постановления Пленума Верховного Суда Российской Федерации по разъяснению законодательства об уголовной ответственности за преступления в сфере компьютерной информации, а также иные преступления, совершенные с использованием электронных или информационно-телекоммуникационных сетей.

Постановление Пленума призвано устранить пробелы в правоприменительной практике, включая определение понятия компьютерной информации и действий, составляющих преступления в этой области. Постановление разъясняет, что считается охраняемой законом компьютерной информацией и какие действия признаются неправомерным доступом к ней.

Постановление как раз и должно нивелировать сложности в правоприменительной практике, так как они возникали даже с тем, что именно относить к компьютерной информации.

¹ Уголовный кодекс Республики Казахстан от 16 июля 1997 г. № 167. URL: <https://adilet.zan.kz/> (дата обращения: 06.03.2024).

² Российская газета. 2022. 28 дек.

В примечании к ст. 272 УК РФ указано, что под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. Однако это определение не вносило ясности относительно такого критерия компьютерной информации, как «охраняемая законом». Встречалось мнение, что доступ к компьютерной информации является неправомерным, если осуществляется в нарушение порядка, установленного российским законодательством, в частности, законами о государственной тайне, о персональных данных, о коммерческой тайне, о банках и банковской деятельности и др.

В пункте 3 постановления Пленума Верховного Суда разъясняется, что по смыслу ч. 1 ст. 272 УК РФ под охраняемой законом компьютерной информацией следует понимать:

– информацию, для которой законом установлен специальный режим правовой защиты, ограничен доступ, введены условия отнесения ее к сведениям, составляющим государственную, коммерческую, служебную, личную, семейную или иную тайну (в том числе персональные данные), установлены обязательность соблюдения конфиденциальности такой информации и ответственность за ее разглашение;

– информацию, для которой правообладателем установлены средства ее защиты, направленные на обеспечение ее целостности или доступности.

Кроме того, разъяснения, касающиеся определений, даны в пп. 17 и 18 постановления. В них указано следующее:

– под информационно-телекоммуникационной сетью в соответствующих статьях Особенной части УК РФ понимается технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;

– под сетью «Интернет» понимается всеобщая информационно-телекоммуникационная сеть, объединяющая информационные системы и сети электросвязи различных стран и предоставляющая возможность реализации раз-

личных форм связи между пользователями, в том числе размещения информации, доступной для неограниченного круга лиц.

Важные разъяснения касаются действий, составляющих объективную сторону составов преступлений, предусмотренных в вышеперечисленных статьях главы 28 УК РФ. Пленум Верховного Суда дал толкование:

- что является уничтожением, блокированием, модификацией, копированием компьютерной информации;
- что понимать под нейтрализацией средств защиты компьютерной информации (п. 4);
- какие действия считаются неправомерным доступом к компьютерной информации (п. 5).

Эти разъяснения позволят более четко разделять и квалифицировать совершенные действия.

Ранее суды могли ошибочно вменить несколько способов при одном фактически совершенном действии (например, при видоизменении кода программы путем снятия ключа блокировки вменяли модификацию и копирование без описания действий по копированию). И наоборот, при фактическом совершении нескольких действий вменяли один способ.

Это важное решение позволит усилить борьбу с преступлениями в области компьютерной информации и повысить эффективность правоприменительной практики в этой сфере.

Учитывая положительный опыт Пленума Верховного Суда Российской Федерации, который разъясняет и обеспечивает единообразное применение российскими судами законодательства об уголовной ответственности за преступления в сфере компьютерной информации, а также иные преступления, совершенные с использованием электронных или информационно-телекоммуникационных сетей, включая сеть Интернет, его можно признать уголовно-правовой мерой предупреждения киберпреступности. Считаем целесообразным в Республике Казахстан принять аналогичное нормативное постановление Верховного Суда Казахстана.

Таким образом, для правильного понимания прав и обязанностей государств по вопросам международной кибербезопасности предлагаем делить нормативные правовые акты на следующие группы:

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

Указанная классификация законодательства в области обеспечения кибербезопасности, на наш взгляд, будет способствовать правильному построению системы мер предупреждения, обнаружения недостатков в правовом регулировании и отмене повторяющихся нормативных актов, связанных с кибербезопасностью (информационной безопасностью) и киберпреступностью в России и Казахстане.

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

– отсутствует единая система нормативных правовых актов в России и Казахстане, направленных на предотвращение киберпреступности. Создание такой системы возможно только на основании правового регулирования, охватывающего три уровня такого регулирования: 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;

– низкая правовая грамотность населения, сотрудников в сфере ИКТ и руководителей организаций в отношении вопросов информационной безопасности является значительной проблемой.

Наиболее продуктивной представляется ориентация на развитие законодательства о профилактике и противодействии киберпреступности на уровне стран СНГ на основе директивных документов содружества. При этом оптимизацию правового обеспечения предупреждения киберпреступности в Российской Федерации и Республике Казахстан необходимо связывать с достижением баланса регулирования вопросов кибербезопасности на международном, межгосударственном и национальном уровнях. На международном уровне в качестве первоочередной меры необходимы подписание и ратификация нашими странами принятой резолюцией 79/243 Генеральной Ассамблеи от 24 декабря 2024 г. единой международной Конвенции против киберпреступности¹. На межгосударственном уровне в условиях санкционного давления для России особенно актуально принятие единых нормативных актов дружественных для России стран. На национальном уровне для Казахстана значимо 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 целом базовой составляющей мер предупреждения киберпреступлений в Российской Федерации и Республике Казахстан выступает совершенствование их правового обеспечения.

¹ Конвенция против киберпреступности. Укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям. URL: <https://www.un.org/ru/documents/treaty/A-RES-79-243> (дата обращения: 12.04.2025).

§ 3. Меры предупреждения киберпреступлений

Киберпреступность как современная разновидность общественно опасного социального поведения представляет значительную угрозу для безопасности наших государств и требует соответствующего противодействия, включающего в себя не только борьбу уголовно-правовыми средствами с ней, но и предупреждение, направленное на устранение причин, ее порождающих.

В целом предупреждение преступлений (уголовных правонарушений) в широком смысле слова являет собой систему экономических, социально-культурных, воспитательных и правовых мер, осуществляемых органами государственной власти в процессе формирования правового государства и гражданского общества. Предупреждение преступности (правонарушений) выступает особым видом деятельности в области социального управления¹.

Предупреждение преступлений (уголовных правонарушений) в узком смысле – это комплекс предпринимаемых правоохранительными органами специальных мер по недопущению или пресечению криминальных посягательств, осуществляемых различными предусмотренными законом средствами.

В рамках криминологии было представлено глубокое теоретическое обоснование предупреждения преступности, которое стало альтернативой научному подходу уголовного права в формулировке основных целей, задач и мер борьбы с преступностью в современном обществе. Сегодня предупреждение преступности есть главная стратегия государства и общества в противодействии этому негативному социальному явлению.

Мы поддерживаем мнение тех ученых, которые считают, что предупреждение преступности – это сложная система государственных и общественных мер, направленных на выявление, устранение, ослабление или нейтрализацию причин и условий, способствующих совершению преступлений различных видов². Ос-

¹ *Исмагулова А. Т., Галиаскарова А. М.* Уголовные правонарушения в сфере информатизации и связи в Республике Казахстан : монография. Костанай, 2016. С. 124–125.

² *Каиржанов Е. И.* Криминология. Общая часть : учебник для вузов. Алматы, 2000. С. 157.

новная цель таких мер заключается в предотвращении возможности перехода лиц, которые по своим условиям жизни и поведению могут быть склонными к общественно опасным посягательствам, на путь совершения преступлений. Разработка этих мер является основной задачей криминологических исследований, а успешное внедрение их на практике служит показателем эффективности проведенных исследований¹.

Предупреждение преступности представляет собой систему, включающую в себя: объекты и субъекты предупредительной деятельности, а также средства (конкретные меры, инструменты такого воздействия на преступность) и методы предупредительного воздействия.

Предупреждение преступности должно соответствовать принципам законности, гуманизма и справедливости, при этом строиться на научной основе. Для реализации научного подхода к предупреждению преступлений необходима такая последовательность действий, которая включает в себя постановку перед исполнителями обоснованных целей, определение конкретных задач, рассчитанных на возможности имеющихся сил и средств, разработку предупредительных и профилактических мер, опирающихся на соответствующую информационную, методологическую и ресурсную базу. При этом особое внимание уделяется учету специфики условий и ситуаций, характерных для конкретных территорий или сфер социальной жизни.

Научный подход к предупреждению и профилактике преступности также означает:

- тщательный анализ текущих и потенциальных преступных явлений и прогнозирование их развития в обозримом будущем;
- планирование мер предупреждения преступности, правовое регулирование и управление ими на основе понимания закономерностей и роли таких мер в социальных системах;

¹ Долгова А. И. Криминология : учебник. М., 2013. С. 784.

– научно-методическое сопровождение предупредительной деятельности, основанное на комплексном использовании знаний криминологии и уголовной политики в борьбе с преступностью;

– использование закономерностей преступности, выявленных наукой, и возможностей борьбы с ней для точной оценки ситуации в прошлом, настоящем и будущем и принятия обоснованных стратегических и тактических решений¹.

Практическое применение принципа научной обоснованности в деятельности по предупреждению преступности значительно усиливает ее эффективность за счет повышения точности, направленности, своевременности применения и всесторонности воздействия выбранных мер предупреждения преступлений.

Деятельность по предупреждению киберпреступности также должна соответствовать всем вышеупомянутым принципам, для того чтобы обеспечить качественную основу для создания и реализации системы мер предупреждения киберпреступлений.

Так, предупреждение киберпреступности в наших странах должно прежде всего соответствовать принципу законности как определенному режиму общественной жизни, методу государственного руководства обществом, состоящему в организации общественных отношений посредством издания и неуклонного исполнения законов и других правовых актов². Для полноты реализации данного принципа в деятельности по предупреждению киберпреступности должны быть созданы правовые основы противодействия преступности в целом и киберпреступности в частности. Наличие правовых основ предупреждения преступности гарантирует законность в этой сфере общественных отношений, неприкосновенность прав и законных интересов граждан, а также учреждений и организаций, в значительной мере обеспечивает эффективность предупредительных мероприятий.

Правовая база противодействия преступности, в том числе и предупреждения преступности в России и Казахстане, формировалась не один год, и ее совер-

¹ Кузнецова Н. Ф., Лунеев В. В. Криминология : учебник. 2-е изд., перераб. и доп. М., 2004. С. 51–75.

² Криминология. Общая часть : учебник для вузов / Кириллов М. А. [и др.] ; под ред. М. А. Кириллова, В. И. Омигова. Чебоксары, 2010. С. 232.

шенствование продолжается, она представляет собой весьма обширную систему правовых документов, регулирующих процесс борьбы с преступностью¹. В конце XX – начале XXI вв. наши государства предпринимали самостоятельные шаги в целях успешного правового обеспечения деятельности по предупреждению преступности².

Так, в Республике Казахстан на шесть лет раньше, чем в России, был принят Закон РК от 29 апреля 2010 г. № 271-IV «О профилактике правонарушений»³, который определил правовые, экономические, социальные и организационные основы деятельности государственных органов, органов местного самоуправления, организаций и граждан по профилактике правонарушений. В России Федеральный закон «Об основах системы профилактики правонарушений в Российской Федерации»⁴ (далее – Закон о профилактике правонарушений) был принят в 2016 г. и стал основой для развития системы профилактики правонарушений в России⁵. Вместе с тем следует отметить, что в российской юридической литературе высказываются мнения о том, что необходимо и дальше развивать нормативные основы предупреждения преступности, а Закон о профилактике правонарушений является тем актом, который должен решить проблему отсутствия единой системы предупреждения преступлений, причем из его названия ясно, что эта система будет посвящена не только предупреждению преступлений⁶.

В целом следует признать, что в данных законах о профилактике правонарушений Российской Федерации и Республики Казахстан, несмотря на внешнее

¹ Там же. С. 211 ; *Джекебаев У. С.* Преступность как криминологическая проблема. Алма-Ата, 1974. С. 97.

² *Алауханов Е. О.* Криминология : учебник. СПб., 2013. С. 378.

³ *О профилактике правонарушений* : закон Республики Казахстан от 29 апреля 2010 г. № 271-IV. URL: <https://adilet.zan.kz/rus> (дата обращения: 06.02.2023).

⁴ *Об основах системы профилактики правонарушений в Российской Федерации* : федеральный закон от 23 июня 2016 г. Доступ из справ.-правовой системы «КонсультантПлюс».

⁵ *Научно-практический комментарий Федерального закона Российской Федерации от 23 июня 2016 г. № 182-ФЗ «Об основах системы профилактики правонарушений в Российской Федерации»* / под общ. ред. д-ра юрид. наук, проф. В. И. Майорова. Тюмень, 2017.

⁶ *Григор А. А.* Понятия «профилактика» и «предупреждение» преступности в контексте исследования российского законодательства // Проблемы социально-гуманитарного образования на современном этапе модернизации российской школы : мат-лы девятой всерос. науч.-практ. конф. с междунар. участием / под науч. ред. И. И. Макаровой. Барнаул, 2021. С. 130–133.

различие содержания понятий «предупреждение преступности» и «профилактика правонарушений», содержатся основы системы предупреждения различных видов преступлений, в том числе и киберпреступлений¹.

Проблема предупреждения киберпреступности с каждым годом становится более актуальной в наших странах. Ежегодно в Российской Федерации и Республике Казахстан наблюдаются динамика непрерывного роста киберпреступлений, постоянное обновление способов их совершения. Государство, люди, организации вынуждены постоянно совершенствовать собственную кибербезопасность, чтобы не столкнуться с ущербом из-за противоправных деяний². Это ставит перед правоохранительными органами обеих стран актуальную задачу по предупреждению киберпреступлений, что в свою очередь требует своевременного решения ряда насущных проблем. Прежде всего, следует решить задачу предупреждения киберпреступности путем воздействия на наиболее распространенные киберпреступления, начать активную разработку комплекса предупредительных мер, работающих на опережение, учитывающих формирующиеся тенденции киберпреступности³.

Проведенное нами исследование показало, что преступность в сфере компьютерной информации и с использованием информационно-телекоммуникационных технологий в России и Казахстане носит в основном корыстный характер, поэтому при совершенствовании мер предупреждения киберпреступности правоохранительным органам государств необходимо уделять более пристальное внимание решению проблем, связанных с воздействием на детерминанты корыстной киберпреступности. При этом эффективность предупреждения киберпреступности напрямую зависит от учета особенностей внутренних и внешних факторов, влияющих на социально-экономические, организационно-технические, правовые условия, обуславливающие наиболее распространенные

¹ *Карабеков К. О.* Профилактика кибербуллинга в подростковой среде // Защита прав детей: сотрудничество полиции и гражданского общества : мат-лы междунар. науч.-практ. конф. Костанай, 2022. С. 71.

² *Байрамов Р. Р., Пасат В. А.* Анализ киберпреступлений и мер по их предупреждению // Ученые записки Санкт-Петербургского имени В. Б. Бобкова филиала Российской таможенной академии. 2022. № 1(81). С. 63.

³ *Жмыхов А. А.* Компьютерная преступность за рубежом и ее предупреждение : дис. ... канд. юрид. наук. М., 2003. С. 10.

виды киберпреступлений. Структура и содержание детерминант киберпреступности позволяют сформулировать вывод, что ее предупреждение в Российской Федерации и Республике Казахстан должно основываться на учете: внутренних факторов, связанных с национальными социально-экономическими, организационно-техническими, правовыми и организационными условиями развития наших государств, и внешних факторов, связанных с влиянием деятельности зарубежных государств и международных отношений на развитие наших стран¹.

Рассмотрим основные направления разработки мер предупреждения киберпреступности, ориентированные на устранение *внутренних* факторов, определяющих ее существование в современном виде в России и Казахстане, подробнее.

1. Социально-экономические меры предупреждения киберпреступности – это меры, направленные на защиту информационных средств и данных собственников, нейтрализующие действие социальных и экономических факторов, влияющих на активность киберпреступников, т. е. условия возникновения экономических мотивов у последних.

Приоритетными социально-экономическими мерами, способствующими предупреждению киберпреступности в России и Казахстане, являются:

- проведение системной политики кибербезопасности, взаимоувязывающей все ее направления: защиту персональных данных граждан и критическую информационную инфраструктуру;

- проведение кампаний, направленных на повышение 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;

¹ *Карабеков К. О.* Детерминанты и меры предупреждения киберпреступлений в Российской Федерации и Республике Казахстан. С. 357.

– устранение негативных последствий в экономической сфере Российской Федерации с помощью эффективной государственной поддержки малого и среднего бизнеса, а также замещения импортных товаров отечественными. В качестве позитивных последствий социально-экономических мер выступают развитие производственных площадок, появление новых рабочих мест, укрепление отечественного сектора экономики.

Одна из главных общих проблем предупреждения обусловлена, прежде всего, недостаточной осведомленностью населения об опасности киберпреступности и необходимых мерах кибербезопасности. Еще далеко не все знают о высочайшей опасности киберпреступлений, связанной с тем, что практически каждый гражданин в любую минуту может оказаться жертвой киберпреступников. Многие люди не представляют, как защитить свои личные данные и устройства от кибератак. Недостаточное знание о мерах кибербезопасности неизбежно приводит к тому, что человек становится жертвой киберпреступников. Существует необходимость активизировать меры по обучению и повышению осведомленности населения о мерах предупреждения киберпреступлений через проведение семинаров, тренингов и кампаний.

2. Организационно-технические меры предупреждения киберпреступности связаны с разработкой, внедрением, непосредственной реализацией и усовершенствованием технических мер, направленных на обеспечение безопасности в сфере информации и информационных технологий, включая 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 кибербезопасности¹.

Необходимо максимально скоординировать действия всех заинтересованных сторон – правоохранительных органов, предпринимателей, общественных организаций, исследовательских учреждений и граждан – для предупреждения

¹ Там же.

киберугроз. В настоящее время отсутствуют эффективные механизмы противодействия новым видам преступлений в сфере информационных технологий.

В целях автоматического повышения уровня осведомленности граждан о постоянных угрозах, существующих при работе в интернет-пространстве, и правилах пользования интернет-ресурсами необходимо внедрять в программное обеспечение пользовательских действий в сети Интернет дополнительные блоки в виде кратких обучающих курсов, тестов знания основ кибербезопасности, пользовательских соглашений, предваряющих вхождение в сеть Интернет, без обязательного прохождения которых невозможно получение доступа к интернет-ресурсам. Сведения о возможности защиты себя в киберпространстве от воздействия злоумышленников снизят уровень совершаемых киберпреступлений в сфере компьютерной информации и с использованием персональных данных. Кроме того, как специальную меру предлагаем в мобильных приложениях всех банков распространять на постоянной основе короткие видеоролики, содержащие информацию о новых способах совершения интернет-мошенничеств.

Считаем целесообразным разрабатывать меры предупреждения киберпреступлений с учетом виктимологических особенностей потерпевших от интернет-мошенничеств. Для этого во всех крупных учреждениях, организациях и предприятиях (независимо от формы собственности) России необходимо разработать и внедрить образовательно-информационные программы для различных возрастных групп, которые знакомили бы членов коллектива с методами мошенничества и помогали бы работникам развивать навыки самозащиты в интернете. Помимо этого, следует популяризировать меры предосторожности в интернете, распространять соответствующие рекомендации и советы о безопасном поведении в сети.

Необходимо внести изменения в систему защиты персональных данных, чтобы минимизировать количество цифровых следов и персональной информации в интернет-пространстве. Например, в банковские приложения или на сайты, предоставляющие те или иные услуги, для получения которых требуется ввести ФИО, паспортные данные, информацию из медицинского страхового полиса или индивидуальные данные банковской карты, ввести доступ с установкой двухфак-

торной аутентификации. Таким образом сократится количество возможных способов завладения персональными данными или финансовыми элементами, так как при попытке воспользоваться сервисами интернет-ресурса лицу предстоит доказать правомерность доступа.

Необходимо внедрение новых специализаций в образовательный процесс юридических вузов, особенно для курсантов и слушателей образовательных учебных организаций правоохранительной системы Российской Федерации и Республики Казахстан. Государственные гранты должны быть предоставлены для проведения актуальных виктимологических и криминологических исследований киберпреступности, которые направлены на выявление объективных закономерностей, факторов киберпреступности, характеристик отдельных типов личности киберпреступников и различных аспектов обеспечения кибербезопасности¹.

Считаем целесообразным разработку и внедрение современных технических средств защиты информации, включая фреймворки, шифрование данных, средства мониторинга и обнаружения аномалий². Необходимо усиление мер по обеспечению кибербезопасности критической информационной инфраструктуры, в том числе государственных систем управления и контроля, банков, крупных предприятий и организаций. Требуется регулярное проведение аудитов и испытаний систем информационной безопасности, чтобы выявить и поправить уязвимости и слабые места.

Указанные меры не исчерпывают всего перечня действий, но позволяют эффективно защищать свои цифровые ресурсы и инфраструктуру.

3. Организационно-управленческие меры предупреждения киберпреступности предусматривают внедрение формализованных принципов стратегического противодействия киберугрозам, направленных на оптимизацию соответствующих ответных действий и создание специализированных подразделений для быстрого раскрытия и расследования имущественных киберпреступлений по типу

¹ Старостенко О. А. Профилактика и предупреждение кибермошенничества // Наука. Образование. Современность. 2020. № 1–2. С. 41–44.

² Рустемова Г. Р. Профилактика уголовных правонарушений в сфере информатизации и связи в Республике Казахстан // Вестник Могилевского института МВД. 2020. № 1. С. 61.

«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 преступлений¹.

Изучение положительного опыта предупредительной деятельности России и Казахстана показывает, что в практической деятельности правоохранительных органов наших стран принимается ряд важных для государств организационно-управленческих мер предупреждения киберпреступности, направленных в том числе и на предупреждение киберпреступлений против собственности.

Так, в Российской Федерации государственными органами и специализированными службами, такими как Федеральная служба безопасности (ФСБ), Министерство внутренних дел (МВД) и Министерство цифрового развития, связи и массовых коммуникаций (Минцифры), выявляются, расследуются и предупреждаются киберпреступления. Развивается сотрудничество между государственными органами, бизнес-сектором и общественностью для обмена информацией, повышения кибербезопасности и координации действий по предупреждению киберпреступлений.

В Российской Федерации функционирует Управление «К» Бюро специальных технических мероприятий МВД. Основными направлениями его деятельности являются борьба с преступлениями в сфере компьютерной информации, пресечение противоправных действий в информационно-телекоммуникационных сетях (включая сеть Интернет), борьба с незаконным оборотом радиоэлектронных и специальных технических средств, выявление и пресечение нарушений авторских и смежных прав в сфере информационных технологий, борьба с международными преступлениями в сфере информационных технологий и международное

¹ *Карабеков К. О.* Детерминанты и меры предупреждения киберпреступлений в Российской Федерации и Республике Казахстан. С. 357.

сотрудничество в борьбе с преступлениями, совершаемыми с использованием информационных технологий¹.

В борьбе с имущественными киберпреступлениями правоохранительным органам следует использовать накопленный организационный и тактический опыт борьбы подразделений по контролю за оборотом наркотиков и Роскомнадзора.

Так, в целях борьбы с распространением наркотиков в интернете Главное управление по контролю за оборотом наркотиков МВД России (ГУНК МВД России) и Роскомнадзор активно осуществляют мониторинг сети, выявляя и пресекая работу множества интернет-ресурсов, которые пропагандируют употребление наркотиков и продажу наркосодержащих препаратов. Более того, эти ресурсы также занимаются финансовыми операциями, включая вывод денег, полученных с помощью незаконной торговли наркотиками за рубежом. Основная часть этих ресурсов имеет регистрацию за пределами Российской Федерации, что создает проблемы в полном пресечении их деятельности и привлечении организаторов наркобизнеса к ответственности. Нынешний государственный механизм ограничения доступа к этим сайтам отстает от развития технологий, позволяющих скрыть или изменить IP-адрес компьютера пользователя, обеспечивая свободный доступ к запрещенным на территории России сайтам. В связи с этим большинство продаж наркотиков осуществляется через анонимные онлайн-рынки или так называемую «темную сеть»².

ГУНК МВД России постоянно выявляет и информирует своих сотрудников об актуальных бесконтактных схемах сбыта наркотиков, которые создают значительные проблемы при выявлении, документировании и доказывании наркопреступлений. Особую опасность представляют специализированные форумы, включая социальные сети, где обсуждаются вопросы употребления наркотиков. Здесь происходит интенсивный обмен информацией среди наркозависимых о методах

¹ Новые способы совершения преступлений в сфере информационных технологий на территории государств – участников СНГ : аналитический обзор / И. Б. Колчевский, В. М. Журавлев, А. Г. Кузнецов и О. В. Демковец, Д. А. Брехов. М., 2018. С. 17.

² Там же.

изготовления, культивации, приема и местах приобретения наркотических средств, а также о правилах поведения при задержании правоохранительными органами. Помимо анонимных онлайн-ресурсов, даркнета, торговые площадки сбывают разнообразные наркотики в России, Беларуси, Украине и Казахстане, используя для сделок и оплаты исключительно биткойны.

В органах внутренних дел Республики Казахстан задачи по противодействию преступлениям в сфере информатизации и связи и с использованием информационных технологий отнесены к компетенции Центра по борьбе с киберпреступностью (далее – Центр) Департамента криминальной полиции МВД и его территориальных подразделений¹. Основным направлением работы Центра и его территориальных подразделений выступает борьба с преступлениями в виртуальном пространстве, а также организация работы по выявлению, пресечению и раскрытию преступлений в сфере информационных технологий и преступлений, совершаемых с их использованием, таких как: 1) преступления в сфере информатизации и связи (глава 7 УК РК, предусматривает 9 составов преступлений); 2) незаконное распространение порнографии (в том числе с участием несовершеннолетних), культа жестокости и насилия, совершаемых и с использованием ресурсов сети Интернет; 3) борьба с распространением контрафактной продукции; 4) сбыт специальных технических средств; 5) электронные хищения и т. д.²

Кроме того, с учетом специальных познаний и накопленного опыта сотрудниками подразделений по борьбе с киберпреступностью проводятся мероприятия по раскрытию иных преступлений, совершаемых с использованием информационных технологий, таких как оскорбление, распространение заведомо ложной информации в сети Интернет и т. д.

¹ Официальный сайт Министерства внутренних дел Республики Казахстан (МВД РК). URL: <https://www.gov.kz/memleket/entities/qriim> (дата обращения: 28.02.2022).

² Карабеков К. О. Опыт Республики Казахстан по борьбе с киберпреступностью // Преемственность и новации в юридической науке : мат-лы всерос. науч. конф. адъюнктов, аспирантов и соискателей. Омск, 2022. Вып. 18. С. 58.

Наиболее распространенными киберпреступлениями в Республике Казахстан являются интернет-мошенничества. Данная проблема актуализируется тем, что масштабы данных преступлений постоянно растут. Интернет-мошенничества представляют серьезную угрозу для бизнеса и населения. Одной из наиболее часто применяемых форм кибермошенничества выступает фишинг, т. е. метод атаки, когда злоумышленник отправляет ложные электронные письма, в которых просит пользователей предоставить свои личные данные, пароли или банковские реквизиты.

Еще одна распространенная форма кибермошенничества – мошенничество с использованием банковских карт, когда злоумышленники получают доступ к банковским картам путем взлома сайтов или установки вредоносных программ на компьютеры пользователей.

Для предотвращения интернет-мошенничества в Республике Казахстан принимаются организационно-управленческие меры. Так, в 2018 г. был создан Национальный координационный центр информационной безопасности (НКЦИБ)¹. В Республике Казахстан действует Закон «О персональных данных и их защите»², который регулирует сбор, хранение и использование персональных данных граждан. Сотрудники НКЦИБ осуществляют деятельность по выявлению угроз и инцидентов информационной безопасности в казахстанском сегменте сети Интернет в круглосуточном режиме. В рамках сотрудничества с международными организациями НКЦИБ выстроено взаимодействие по реагированию и устранению угроз / инцидентов информационной безопасности. НКЦИБ является членом 6 профильных международных организаций: FIRST, APWG, TF-CSIRT, OIC-CERT, CAMP и APCERT.

Подписаны меморандумы о взаимопонимании в области кибербезопасности с 17 профильными службами таких стран, как Франция (THALES), Российская Федерация (Positive Technologies, Kaspersky Lab), Израиль (Check Point, INCD),

¹ URL: <https://sts.kz/achievements-nkcib/> (дата обращения: 28.02.2022).

² *О персональных данных и их защите* : закон Республики Казахстан от 21 мая 2013 г. № 94-VI. URL: <https://adilet.zan.kz/> (дата обращения: 28.02.2022).

Малайзия (Cyber Security Malaysia), Беларусь (ОАЦ при Президенте РБ), Туркменистан, Бангладеш (BGD e-GOV CIRT), Китай (CNCERT/CC), Болгария (CERT.BG), Грузия (CERT.GOV.GE), Индонезия (ID-CERT), Азербайджан (CERT.GOV.AZ), Узбекистан (UZCERT), Республика Молдова (CERT-GOV-MD), Объединенные Арабские Эмираты (aeCERT), Япония (JPCERT/CC), Украина (CERT-UA)¹.

НКЦИБ в целях развития взаимодействия с оперативными центрами информационной безопасности (ОЦИБ) были реализованы мероприятия, направленные на повышение эффективности взаимодействия в части реагирования на угрозы информационной безопасности и инциденты с ней, проведены встречи по ознакомлению с деятельностью НКЦИБ, по вопросам лицензирования деятельности ОЦИБ, по использованию веб-платформы НКЦИБ и другим вопросам.

Однако, несмотря на принимаемые меры, количество случаев интернет-мошенничества продолжает расти. Это связано с тем, что злоумышленники постоянно развивают новые методы атак и находят уязвимости в системах безопасности.

В работе правоохранительных органов Казахстана встречаются определенные проблемы, связанные с использованием различных социальных сетей, таких как Facebook², Twitter³, ВКонтакте, Одноклассники и др., а также мессенджеров для мобильных телефонов (WhatsApp, Viber, Line и т. д.). Эти платформы часто используются для распространения незаконной информации. Например, на YouTube и WhatsApp пользователи загружают видеоматериалы, содержащие факты насилия, пыток, истязаний, похищения людей, а также ложную информацию, что может вызвать массовые беспорядки и т. д. В то же время такие пользователи

¹ См., напр.: Подписан Меморандум о взаимопонимании в области информационной безопасности между Казахстаном и Азербайджанской Республикой 6 августа 2024 г. URL: <https://gov.kz> (дата обращения: 17.09.2024).

² Принадлежит компании Meta, деятельность которой признана экстремистской и запрещена на территории Российской Федерации

³ На территории Российской Федерации действие заблокировано.

обычно скрывают свою личность, создавая фальшивые профили, или их профили блокируются и удаляются модераторами¹.

Часто граждане обращаются в правоохранительные органы из-за обидных комментариев, включающих признаки разжигания социальной, национальной, религиозной или другой вражды. Однако данные платформы не подчиняются законодательству Республики Казахстан. Любая информация о заинтересованных пользователях может быть получена только по запросу или на основании международного судебного поручения. Особенно сложно установить источник информации на Facebook², Twitter³, WhatsApp, Viber, YouTube, так как они находятся под юрисдикцией иностранных государств.

Казахстан, как и многие другие страны, предпринимает активные шаги по созданию условий для правоохранительных органов по борьбе с киберпреступностью. Одним из примеров современной организации деятельности правоохранительных органов Казахстана является реализация проекта «Ударно-целевая группа „Киберпол“», которая стала прообразом будущих подразделений по борьбе с киберпреступлениями имущественного характера. Цель проекта – это пресечение, раскрытие и расследование имущественных и иных киберпреступлений в Казахстане специализированным подразделением, использующим передовые методы и современные технологии. Для этого группа была обеспечена всем необходимым организационно-техническим оборудованием с широкими техническими возможностями, прямым выходом в сеть Интернет, доступом ко многим банкам данных. В указанное подразделение были включены высококвалифицированные специалисты, обладающие экспертными знаниями в области кибербезопасности, цифрового следствия, мониторинга сетевой активности и других аспектов, связанных с киберпреступностью.

¹ Новые способы совершения преступлений в сфере информационных технологий на территории государств – участников СНГ: аналитический обзор / И. Б. Колчевский, В. М. Журавлев, А. Г. Кузнецов и О. В. Демковец, Д. А. Брехов. С. 18.

² Принадлежит компании Meta, деятельность которой признана экстремистской и запрещена на территории Российской Федерации.

³ На территории Российской Федерации действие заблокировано.

В рамках проекта успешно внедрена система блокировки «зарубежных» звонков с подменных номеров, используемых мошенниками, что позволило пресечь свыше 43 млн попыток таких соединений, вследствие чего количество пострадавших сократилось более чем в 2,5 раза. Эффект работы Киберпола весьма ощутим: в настоящее время раскрыто более 3 тыс. таких преступлений. Сотрудники подразделения «Киберпол» напрямую взаимодействуют с банками и операторами сотовой связи¹.

Организация раскрытия, расследования и предупреждения киберпреступлений имущественного характера с использованием подразделений, специально создаваемых для борьбы с такими преступлениями, является перспективным направлением решения этой трудной задачи для органов внутренних дел России и Казахстана. Это позволяет преодолевать трансграничный характер киберпреступлений, бороться с недостаточным системным анализом следственной и судебной практики, обеспечивать практических работников методическими рекомендациями по организации расследования киберпреступлений.

Для анализа других направлений совершенствования мер по предупреждению киберпреступлений корыстной направленности было проведено анкетирование сотрудников правоохранительных органов России (прил. 3) и Казахстана (прил. 4), которым было предложено указать наиболее эффективные меры для предупреждения киберпреступности (табл. 5).

Указанные данные в таблице 5 свидетельствуют о том, что большая часть сотрудников правоохранительных органов Российской Федерации и Республики Казахстан считает, что повышению эффективности противодействия киберпреступлениям прежде всего будет способствовать привлечение средств массовой информации к пропаганде и систематическому освещению вопросов цифровой грамотности.

¹ Проект «Ударно-целевая группа „Киберпол“» // Официальный сайт МВД РК. URL: <https://www.gov.kz/memleket/entities/-qriim> (дата обращения: 09.02.2024).

Таблица 5 – Ответы сотрудников правоохранительных органов Российской Федерации (268 чел.) и Республики Казахстан (243 чел.) на вопрос «Какие меры, на Ваш взгляд, будут способствовать повышению эффективности противодействия киберпреступлениям?», %

Меры	Доля ответов сотрудников, %	
	РФ	РК
Привлечение средств массовой информации к пропаганде и систематическому освещению вопросов цифровой грамотности	50	49,79
Изменения уголовного законодательства в сторону его упрощения	39,92	—
Осуществление программ просвещения в области защиты личности, общества и государства	39,92	49,79
Правовая поддержка населения	39,92	25,10
Мобилизация организационных ресурсов органов внутренних дел	39,92	12,50
Усиление репрессивных мер в отношении лиц, совершивших киберпреступления	30,22	21,81
Изменение уголовно-процессуального законодательства и законодательства об оперативно-розыскной деятельности в области расширения полномочий правоохранительных органов	30,22	13,16
Проведение периодических оперативно-профилактических мероприятий с привлечением сотрудников других контролирующих органов	19,77	38,27
Привлечение специалистов из IT-сферы	10,07	—

В целом опираясь на эти и другие результаты проведенного нами исследования, в целях улучшения работы подразделений органов внутренних дел Республики Казахстан по борьбе с киберпреступностью предлагаем:

- 1) усовершенствовать работу по мониторингу киберпреступлений;
- 2) высшим учебным заведениям системы МВД совместно с практическими подразделениями разработать программы повышения квалификации следователей (дознавателей) по расследованию дел данной категории;
- 3) обеспечить подразделения научно-методической литературой по прикладным аспектам расследования киберпреступлений.

Одной из главных проблем организации предупреждения киберпреступности на государственном уровне является недостаточное финансирование мер кибербезопасности. Необходимо увеличить финансирование деятельности государственных органов по организации и применению мер кибербезопасности, чтобы

создать разветвленную и эффективную систему мер предупреждения киберпреступлений.

Отдельная проблема, напрямую связанная с недостаточным финансированием, состоит в том, что в системе МВД России и Казахстана на данный момент недостаточно обученных специалистов в области IT-технологий, способных участвовать в противодействии киберпреступности. По итогам анкетирования, всего 10,44% сотрудников правоохранительных органов России свой уровень знаний в сфере киберпреступности оценили как высокий; 59,70% – как средний; 29,85% – низкий (прил. 3). Свой уровень знаний в сфере киберпреступности считают средним 89,71% сотрудников правоохранительных органов Казахстана, низким – 1,64%, а остальные 8,64% затруднились с ответом (прил. 4).

Проблемой является и ненадлежащее сотрудничество между государственными органами и частными компаниями в области кибербезопасности. Частные компании имеют большое количество информации о своих клиентах, что может быть полезным для предотвращения киберпреступлений. Однако без сотрудничества с государственными органами эта информация не может быть использована для борьбы с киберпреступниками.

Законодательное разрешение для негосударственных организаций, таких как народные дружины (кибердружины), частные охранные предприятия и частные детективные агентства, иметь в штате технических специалистов и программное обеспечение для выявления и блокирования противоправного контента в информационно-коммуникационных сетях имеет несколько преимуществ¹. Во-первых, это расширит базу экспертов и специалистов в области кибербезопасности. Существенное увеличение числа людей, занимающихся противодействием киберпреступности, поможет более эффективно бороться с новыми угрозами и технологиями, используемыми киберпреступниками. Во-вторых, негосударственные организации могут быть более гибкими и оперативными в своей

¹ Евдокимов К. Н. К вопросу о совершенствовании системы противодействия технотронной преступности в Российской Федерации // Российский следователь. 2021. № 10. С. 69–72.

работе. В отличие от государственных структур, они могут быстрее реагировать на угрозы и преступления благодаря меньшему объему бюрократии.

В-третьих, с участием негосударственных организаций будет усилена конкуренция, что приведет к повышению качества услуг и снижению их стоимости. Участие коммерческих организаций особенно важно для защиты конфиденциальной информации и информационных систем компаний, так как они обладают специализированными знаниями и опытом в этой области.

Дополнительно необходимо учесть некоторые риски и ограничения при привлечении негосударственных организаций к противодействию киберпреступности. Существует опасность злоупотребления полномочиями и нарушения прав частных лиц, а также утечки конфиденциальной информации. Поэтому необходимо разработать строгое законодательство, регулирующее деятельность негосударственных организаций, а также установить механизмы контроля и ответственности за возможные нарушения.

В целом расширение сферы деятельности негосударственных правоохранительных организаций в области кибербезопасности может существенно повысить эффективность предупреждения киберпреступности. Необходимо также тщательно продумать и регламентировать этот процесс, чтобы минимизировать риски и обеспечить соблюдение прав и свобод граждан¹.

Рассмотрим основные направления разработки мер предупреждения киберпреступности, ориентированные на устранение **внешних** факторов, определяющих ее существование в современном виде в России и Казахстане, подробнее².

Международные ограничительные меры связаны с пресечением негативного влияния на наши страны различной деятельности недружественных государств, прежде всего с нейтрализацией деятельности киберпреступных группиро-

¹ Карабеков К. О. Роль кибердружин в противодействии интернет-угрозам // Современные тенденции развития юридической науки : мат-лы междунар. науч.-теор. конф. молодых ученых, посвященной Дню казахстанской науки. Караганда, 2022. С. 38.

² Карабеков К. О. Детерминанты и меры предупреждения киберпреступлений в Российской Федерации и Республике Казахстан. С. 357.

вок и хакеров, которые используют свои навыки и ресурсы для совершения киберпреступлений, а также с противодействием установленным против России санкциям в различных сферах деятельности 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 раза¹.

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

Важным направлением должно стать импортозамещение в секторах экономики, позволяющее сохранить основу ведения бизнеса, а также переориентация торговли товарами на дружественные страны, что позволит обеспечить нормальные темпы роста экономики наших стран, избежать роста безработицы как значительного фактора, провоцирующего совершение большинства киберпреступлений имущественного характера.

Международные организационные меры предусматривают консолидацию усилий правоохранительных органов различных государств по их взаимодействию, а также создание межгосударственных специальных органов, обеспечивающих такое взаимодействие в борьбе с киберпреступностью и ее предупреждение².

¹ URL: <https://www.gov.kz/memleket/entities/qriim/activities/> (дата обращения: 21.01.2025).

² Лопатина Т. М. Криминологические и уголовно-правовые основы противодействия компьютерной преступности : дис. ... д-ра юрид. наук. М., 2006. С. 21.

Выявленные особенности киберпреступности явно демонстрируют, что эффективное противодействие ей внутри отдельных государств невозможно без опоры на активное международное сотрудничество.

На сегодняшний день основные усилия в борьбе с киберпреступностью предпринимаются такими организациями, как Международное многостороннее партнерство против киберугроз (SHRAST), являющееся исполнительным органом в области кибербезопасности ООН и объединяющее усилия ряда государств, неправительственных организаций и экспертов в области информационной безопасности; Международный альянс по обеспечению кибербезопасности (ICSPA), который объединяет правоохранительные органы, включая Европол, международный бизнес и правительства из различных стран мира (например, Австралии, Великобритании, Канады, Новой Зеландии, США и др.); Интерпол, играющий важную роль в обеспечении быстрой и эффективной связи между государствами и этой международной организацией при осуществлении международного розыска и регистрации преступников¹.

Задачи данных организаций заключаются в разработке всеобщих стандартов киберпреступности, которые подлежат уголовному преследованию и отличаются в разных странах, установлении единой терминологии и концептуального аппарата, предоставлении консультационной поддержки на национальном уровне².

Ежегодно возрастает количество служб и ведомств, создаваемых в зарубежных странах в целях противодействия киберпреступности. Например, в США были созданы такие организации, как US Cyber Command – военное подразделение, занимающееся кибербезопасностью, United States Computer Emergency Readiness Team – национальное подразделение по киберзащите в Департаменте внутренней безопасности, Computer Crime and Intellectual Property Section – подразделение, отвечающее за борьбу с компьютерными преступлениями и интеллектуальной соб-

¹ Кильмаматова Э. Р. Международное регулирование преступлений в сфере кибертерроризма // Современные вопросы государства, права, юридического образования : сб. науч. тр. по мат-лам XV междунар. науч.-практ. конф. Тамбов, 2020. С. 334–340.

² Мороз Н. О. Деятельность Интерпола по координации сотрудничества в борьбе с преступностью в сфере высоких технологий // Вестник Полоцкого государственного университета. Серия D «Экономические и юридические науки». 2011. № 14. С. 147.

ственно, а также Internet Police – организация, занимающаяся обеспечением безопасности в сети Интернет. В Великобритании существует Национальный отдел по борьбе с высокотехнологической преступностью, в Австралии – Группа координации безопасности электронной почты (ESCG), в Японии – Федеральное агентство по содействию технологиям, а в Эстонии с 2006 г. функционирует Группа реагирования на чрезвычайные ситуации в области компьютерной безопасности (CERT-EE). В Гааге с 2013 г. действует Европейский центр по борьбе с киберпреступностью, подчиненный Европолу и решающий оперативные и аналитические задачи для борьбы с киберпреступлениями на территории стран Европейского союза, занимающийся взаимодействием с международными партнерами¹.

Россия также следует этому пути. В 2015 г. по поручению Совета безопасности РФ Центральный банк организовал Финансово-информационный центр по борьбе с киберугрозами (FinCERT). Основная задача этого центра – сбор информации о кибератаках на банки и их клиентов, потенциальных угрозах, а также распространение собранных данных по финансовым учреждениям. На 1 октября 2016 г. уже 90 из 716 банков, действующих в России, добровольно предоставляли информацию о воровстве денег со счетов клиентов.

Борьба с киберпреступностью является одной из наиболее актуальных и сложных проблем в криминологии. Высокая скрытность подобных преступлений, постоянный рост числа киберпреступников, развитие информационных технологий, которые предоставляют новые возможности для совершения таких преступлений, требуют новых подходов к противодействию. Киберпреступления, совершаемые в виртуальном пространстве, создают угрозы не только для глобальных информационных сетей, но и для общества в целом².

Поскольку в настоящее время ни одно государство не может защитить себя полностью от кибератак, применяя лишь национальные законодательные меры, необходимо организовать и провести комплексное противодействие киберпре-

¹ Старостенко О. А. Указ. соч. С. 41–44.

² Леонова А. А., Архипов М. Е., Оюн А. С., Шумская В. А. Актуальные вопросы профилактики правонарушений, совершаемых с использованием дистанционных технологий // Правовая позиция. 2023. № 5(41). С. 57–62.

ступности, которое включает: 1) согласование уголовного законодательства относительно киберпреступлений; 2) разработку и внедрение на международном уровне процессуальных стандартов, позволяющих эффективно расследовать преступления в глобальных информационных сетях¹; 3) международное сотрудничество правоохранительных органов при расследовании киберпреступлений на оперативном уровне; 4) эффективный механизм разрешения юрисдикционных вопросов в киберпространстве.

Международно-правовое сотрудничество является важным шагом в преодолении правового вакуума, который возникает между развитием информационных технологий и реагированием законодательства на них².

В завершение отметим, что в настоящем параграфе нами предложен комплекс мер предупреждения киберпреступности в Российской Федерации и Республике Казахстан, который на межгосударственном и государственном уровнях учитывает общественную опасность и негативную динамику наиболее распространенных киберпреступлений, совершаемых в данных странах, и обеспечивает соответствие мер предупреждения сферам действия внутренних и внешних детерминант киберпреступности³.

На государственном уровне это меры, направленные на нейтрализацию внутренних факторов, обуславливающих совершение киберпреступлений. К ним относятся прежде всего социально-экономические меры, такие как 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 рас-

¹ Романенко А. С. Некоторые аспекты борьбы с киберпреступностью // Уголовный закон Российской Федерации: проблемы правоприменения и перспективы совершенствования : мат-лы всерос. круглого стола. Иркутск, 2015. Вып. 6. С. 196.

² Журавленко Н. И., Шведова Л. Е. Проблемы борьбы с киберпреступностью и перспективные направления международного сотрудничества в этой сфере // Общество и право. 2015. № 3(53). С. 70.

³ Карабеков К. О. Детерминанты и меры предупреждения киберпреступлений в Российской Федерации и Республике Казахстан. С. 357.

следования данных преступлений; разработка инструментов для онлайн-обнаружения планируемых, осуществляемых и уже совершенных киберпреступлений, а также лиц, к ним причастных.

Второе место занимают организационно-технические меры. Среди них наиболее актуальны: 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 трансграничного характера.

На третьем месте находятся организационно-управленческие меры: внедрение формализованных принципов стратегического противодействия киберугрозам, направленных на оптимизацию соответствующих ответных действий; создание специализированных подразделений для быстрого раскрытия и расследования имущественных 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.

На межгосударственном уровне это меры, направленные на сокращение и нейтрализацию внешних факторов, обуславливающих совершение киберпреступлений в Российской Федерации и Республике Казахстан. К ним относятся прежде всего 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 изучения новых форм киберпреступлений, законодательных решений, касающихся обеспечения безопасности информационных

сетей; участие в международных форумах, конференциях и совещаниях по выработке мер координации действий по предотвращению киберугроз.

В целом, характеризуя особенности основных направлений предупреждения киберпреступлений в изучаемых странах, для России следует выделить принятие мер, направленных на нейтрализацию влияния внешних факторов, связанных с применением зарубежных санкций, путем разработки собственного технического и программного компьютерного обеспечения, а для Казахстана – принятие мер, направленных на снижение уровня безработицы среди молодого населения.

ЗАКЛЮЧЕНИЕ

Проведенное исследование криминологического состояния киберпреступности в Российской Федерации и Республике Казахстан, мер ее предупреждения в данных странах и полученные при этом результаты позволили сформулировать следующие выводы.

1. Киберпреступность – новое разноформатное общественно опасное явление, к стремительному развитию которого в Российской Федерации и Республике Казахстан правоохранительные органы в целом в свое время оказались не готовы. На государственных уровнях обеих стран принимались меры по его предупреждению, однако уровень теоретического осмысления проблемы, законодательного регулирования, а также предупредительной и профилактической деятельности правоохранительных органов отставал от темпов роста преступной деятельности в киберпространстве.

2. В целях дальнейшего совершенствования системы мер предупреждения киберпреступлений, устранения неопределенности понятийного аппарата нами уточнено определение **киберпреступности** и **содержание ее признаков**. В целом с акцентом на ее фактическое содержание под киберпреступностью в Российской Федерации и Республике Казахстан следует понимать негативное социальное явление уголовно-правового характера, определяемое совокупностью разнородных преступлений (уголовных правонарушений в Казахстане), имеющих особую поведенческую природу образования, включающую в себя общественно опасное использование компьютерной информации и информационно-телекоммуникационных технологий в целях удовлетворения потребностей чаще всего корыстной направленности.

3. Характеризуя состояние рассматриваемых преступлений, мы установили, что уровень, структура и динамика киберпреступности в Российской Федерации и Республике Казахстан имеют не только общие черты, но и существенные отличия.

Отличие проявляется, прежде всего, в доле киберпреступлений в общей массе всей преступности в изучаемых странах: в Российской Федерации эта доля

значительно больше, чем в Республике Казахстан. Так, если в России в 2024 г. доля киберпреступлений в общей структуре зарегистрированных преступлений составляла 40,0%, то в Казахстане она была почти в два раза меньше – 18,9%. Причем эта доля постоянно увеличивается.

Это касается и темпов роста киберпреступности в изучаемых странах. Здесь наблюдается обратная пропорция: в Республике Казахстан данная доля росла более высокими темпами, чем в Российской Федерации. Так, если в России с 2016 г. доля киберпреступлений в общей структуре зарегистрированных преступлений увеличилась в 8 раз, то в Казахстане – в 79 раз.

В Российской Федерации и Республике Казахстан общая структура киберпреступности характеризуется двумя группами преступлений: киберпреступления (уголовные правонарушения) в сфере компьютерной информации (в Казахстане – в сфере информатизации и связи) и киберпреступления, совершаемые с использованием информационно-коммуникационных технологий, среди которых лидирующее место и в России, и в Казахстане занимает вторая группа. Так, в России киберпреступления в сфере компьютерной информации в структуре общей киберпреступности составляют 13,82%, а в Казахстане – 0,28%. При этом существуют противоположные тенденции по изменению доли указанных преступлений. Если в России за прошлый год такая доля по сравнению с предыдущим годом увеличилась, причем в два раза, то в Казахстане она, наоборот, незначительно, но уменьшилась.

Отличаются в изучаемых странах и виды наиболее распространенных киберпреступлений. В России в структуре киберпреступности наиболее распространены такие виды киберпреступлений, как 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 Казахстане распространенным видом уголовных правонарушений в структуре киберпреступности является мошенничество (89,97%). Тем самым нами констатируется корыстный характер киберпреступности в обеих странах в целом.

4. В Российской Федерации структуру киберпреступности на 64% составляют интернет-мошенничества и киберкражи, личность киберпреступника характеризуют закономерности преступного поведения интернет-мошенников и киберворов, которые нужно учитывать при разработке мер предупреждения. В Республике Казахстан структуру киберпреступности на 89,97% составляют интернет-мошенничества, личность киберпреступника характеризуют закономерности преступного поведения интернет-мошенников, которые нужно учитывать при разработке мер предупреждения. Исходя из этого на территории России предупреждение киберпреступлений необходимо осуществлять посредством приоритетной борьбы с мошенничествами и кражами, а на территории Казахстана – с мошенничествами.

5. Первоначальная гипотеза о том, что в стране, где высокий уровень цифровизации, должен быть и высокий уровень киберпреступности, не подтвердилась. Несмотря на высокий уровень цифровизации в Республике Казахстан, данные свидетельствуют о более низком уровне киберпреступности в этой стране по сравнению с Российской Федерацией. Меньший уровень киберпреступности в Казахстане можно объяснить определенным опытом организации работы правоохранительных органов. Для противодействия преступности в сфере информатизации и связи и в сфере использования информационных технологий в Республике Казахстан внедрен проект «Киберпол», реализованный в рамках исполнения поручения Президента Республики Казахстан и масштабированный по всем регионам страны.

6. Анализ основных криминологических характеристик личности киберпреступника в России и Казахстане позволил выявить социально-демографические, нравственно-психологические, уголовно-правовые качества личности современного киберпреступника в обеих странах. С учетом этого предложена классификация лиц, занимающихся киберпреступлениями, основанная на степени их вовлеченности в преступную деятельность: начинающие, устойчивые и профессиональные киберпреступники. Начинающие киберпреступники в общей массе составляют около половины всех киберпреступников, располагают средним уров-

нем дохода и обладают способностью использовать одно или несколько компьютерных устройств. Как правило, это мужчины с базовым образовательным уровнем, их профессиональная деятельность часто связана с информационными технологиями, хотя некоторые из них не имеют постоянной работы. Устойчивые киберпреступники имеют средний или выше среднего уровень дохода и углубленные знания в области информационных технологий. Преимущественно мужчины, хотя наблюдается тенденция к увеличению активности женщин. Обычно они обладают высшим техническим образованием и способны использовать инновационные компьютерные системы. Профессиональные киберпреступники составляют не больше 10% от общего числа киберпреступников, отличаются высоким уровнем материального благосостояния, 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.

7. В рамках исследования нами определены особенности личности российских и казахстанских киберпреступников, совершающих преступления с использованием информационно-телекоммуникационных технологий, среди которых наиболее многочисленной группой являются **кибермошенники** и **киберворы**. В России данная группы киберпреступников характеризуется повышенным уровнем корыстных устремлений в сочетании с отсутствием постоянного источника дохода при нормальной трудоспособности, значительным профессионализмом в использовании ИТ-технологий для достижения преступных целей, отсутствием явного криминального прошлого, наличием определенного жизненного опыта, о чем свидетельствуют возраст от 30 до 49 лет и среднее профессиональное образование, наличием навыков психологического воздействия, выстраивания доброжелательных отношений с собеседниками. Лица, совершающие кибермошенничества в Казахстане, – это, как правило, мужчины, граждане Республики Казахстан, в возрасте от 21 года до 29 лет, имеющие среднее специальное образование, неработающие. Они в среднем на 15 лет младше, чем кибермошенники в России.

8. В ходе исследования определены также особенности характеристики личности преступников, совершающих преступления в **сфере компьютерной информации** в России и уголовные правонарушения в **сфере информатизации и связи** в Казахстане. В России указанным преступникам свойственны желание легкой наживы, преобладание индивидуализма при совершении киберпреступлений, приверженность к определенному способу, специализации в использовании ИТ-технологий при наличии многообразия способов совершения киберпреступлений, постоянное проживание в данной местности, молодой возраст от 18 до 24 лет, наличие среднего профессионального образования, работа в сфере информационных технологий. В **Казахстане** чаще всего это мужчины, граждане Республики Казахстан, находящиеся в возрасте от 21 года до 39 лет, имеющие среднее специальное образование, в большинстве своем (81% случаев) нигде не работающие.

9. На основании анализа современного состояния киберпреступности определено, что **предполагаемые направления развития киберпреступности** будут связаны с активным использованием возможностей искусственного интеллекта, которые облегчают доступ в эту сферу лиц, не обладающих большими техническими знаниями, позволяя даже начинающим преступникам организовывать сложные схемы мошенничества, осуществлять значительные кибератаки. Спрогнозировано появление новых сценариев киберпреступлений, связанных с преодолением языковых и видеобарьеров, изменением контента для усложнения идентификации преступника, созданием фальсифицированного контента для вымогательства, усилением методов манипулирования сознанием, расширением спектра преступлений, совершаемых с использованием ИТ-технологий, и увеличением масштабов кибератак.

10. Рассматривая **комплекс детерминирующих факторов** киберпреступности в России и Казахстане, мы определили ряд важных **внутренних и внешних детерминант** киберпреступности в указанных странах. Внутренние детерминанты киберпреступности мы предлагаем разделять на социально-экономические, организационно-технические, организационно-правовые и организационно-управленческие. При этом в рамках **внутренних социально-экономических де-**

терминант мы выделили наиболее значимые факторы, такие как недостаточное соблюдение мер информационной безопасности на фоне широкого использования информационно-коммуникационных технологий в обществе; несоответствие между потребностями населения в информационных услугах и качественном программном обеспечении и их недоступностью из-за низкого уровня жизни. **Организационно-технические** детерминанты включают следующие наиболее активные факторы: недостаточную защиту информационных систем, уязвимость программного обеспечения, отсутствие эффективных механизмов контроля и обнаружения кибератак. **Организационно-правовые** детерминанты охватывают недостаточное урегулирование на международном и национальном уровнях вопросов кибербезопасности, неразработанность актуальных терминов кибербезопасности и его производных, отсутствие эффективной правовой защиты. Среди **организационно-управленческих** детерминант определены 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 содержат наиболее приоритетные факторы **организационно-технического** (деятельность международных киберпреступных группировок и отдельных хакеров; распространение вредоносного программного обеспечения и технологий, разработанных в других странах) и **организационно-правового** характера (недостатки международно-правового регулирования вопросов предупреждения киберпреступности; сложности в международном сотрудничестве в расследовании и раскрытии киберпреступлений).

11. Результаты научного исследования позволили заключить, что важной составляющей организации предупреждения киберпреступлений является совершенствование его **правового обеспечения**: 1) необходима единая система нормативных правовых актов в Российской Федерации и Республике Казахстан,

направленных на предотвращение киберпреступности; 2) исходя из опыта Казахстана, для систематизации государственной политики в области кибербезопасности необходимо разработать концепцию кибербезопасности Российской Федерации; 3) закрепление конкретных прав и обязанностей государств по вопросам международной кибербезопасности должно быть реализовано на глобальном уровне; 4) ООН как международная организация коллективной безопасности должна предложить государствам адекватные правовые и политические инструменты для обеспечения приемлемого уровня кибербезопасности (информационной безопасности); 5) 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; 6) осуществление нарушений субъектами информатизации и пользователями услуг в области информационных и коммуникационных технологий, включая сбор, обработку, хранение и передачу информации в электронной форме, требует установления соответствующего наказания; 7) низкая правовая грамотность населения, сотрудников в сфере информационных и коммуникационных технологий и руководителей организаций в отношении вопросов информационной безопасности является проблемой; 8) стратегии России и Казахстана по обеспечению кибербезопасности имеют схожие цели, так как она стала приоритетным направлением обеспечения национальной безопасности государств, а также критически важных объектов.

12. В целях совершенствования правового обеспечения предупреждения киберпреступности в Российской Федерации и Республике Казахстан необходимо обеспечение баланса регулирования вопросов кибербезопасности на международном, межгосударственном и национальном уровнях. В целом для этого на **международном** уровне необходимы подписание и ратификация нашими странами принятой единой международной Конвенции против киберпреступности. 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 по-

становления 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. Учитывая положительный опыт ГИАЦ МВД России и переход на сервисную модель полиции в Республике Казахстан, в целях обеспечения прозрачности работы перед населением предлагаем размещать ежемесячный аналитический обзор о состоянии киберпреступности в Республике Казахстан на официальном сайте МВД РК.

В целом наиболее продуктивной представляется ориентация уголовно-правовой политики изучаемых стран на развитие законодательства о профилактике и противодействии киберпреступности на уровне стран СНГ на основе директивных документов этого содружества.

13. С учетом выявленных внутренних и внешних детерминант киберпреступности в изучаемых нами странах предлагаем два основных направления применения мер предупреждения киберпреступлений: **государственного и межгосударственного** уровня.

Среди предупредительных мер **государственного** уровня предлагается следующий комплекс мер, направленных на нейтрализацию внутренних факторов, обуславливающих совершение киберпреступлений:

1. Социально-экономические меры: 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, разработку инструментов для онлайн-обнаружения планируемых, осуществляемых и уже совершенных киберпреступлений, а также лиц, к ним причастных.

2. Организационно-технические меры: 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 трансграничного характера.

3. Организационно-управленческие меры: внедрение формализованных принципов стратегического противодействия киберугрозам, направленных на оптимизацию соответствующих ответных действий; создание специализированных подразделений для быстрого раскрытия и расследования имущественных 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.

Среди предупредительных мер **межгосударственного** уровня предлагается следующий комплекс мер, направленных на нейтрализацию внешних факторов, обуславливающих совершение киберпреступлений в Российской Федерации и Республике Казахстан, **ограничительного и организационного** содержания: пресечение прямого влияния недружественных государств, создавшего угрозы кибербезопасности изучаемых стран; нейтрализация косвенного воздействия на состояние кибербезопасности указанных стран; 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 координации действий по предотвращению киберугроз.

При этом для России основным следует считать принятие мер, направленных на нейтрализацию влияния внешних факторов, связанных с применением зарубежных санкций, путем разработки собственного технического и программного компьютерного обеспечения, в то время как для Казахстана актуальным является принятие мер по нейтрализации внутренних факторов путем снижения уровня безработицы среди молодого населения.

14. В дальнейшем тема диссертационного исследования будет разрабатываться в следующих направлениях: выявление новых тенденций киберпреступности в Российской Федерации и Республике Казахстан; определение новых детерминант киберпреступности, установление причин латентности киберпреступлений; создание комплексной системы профилактических мер, направленных на борьбу с преступлениями, совершаемыми с использованием информационно-телекоммуникационных технологий в России и Казахстане.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

Нормативные правовые акты и иные официальные документы

1. *Конституция* Российской Федерации принята всенародным голосованием 12 декабря 1993 г. : с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 г. // Российская газета. – 1993. – 25 дек. ; 2020. – 4 июля. – Текст : непосредственный.

2. *Конституция* Республики Казахстан принята на республиканском референдуме 30 августа 1995 г. – URL: https://adilet.zan.kz/rus/docs/K950001000_history/. – Текст : электронный.

3. *Уголовный кодекс* Российской Федерации от 13 июня 1996 г. № 63-ФЗ. – Доступ из справ.-правовой системы «КонсультантПлюс». – Текст : электронный.

4. *Уголовный кодекс* Республики Казахстан от 3 июля 2014 г. № 226-V ЗРК. – URL: <https://adilet.zan.kz/rus/docs//>. – Текст : электронный.

5. *Конвенция* о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23 ноября 2001 г.) : с изменениями от 28 января 2003 г. – Доступ из справ.-правовой системы «Гарант». – Текст : электронный.

6. *Конвенция* Организации Объединенных Наций против киберпреступности: Укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям : принята резолюцией 79/243 Генеральной Ассамблеей от 24 декабря 2024 г. // Официальный сайт ООН. – URL: <https://www.un.org/ru/documents/treaty/A-RES-79-243>. – Текст : электронный.

7. *Конвенция* Организации Объединенных Наций против транснациональной организованной преступности 2000 г. : принята в Нью-Йорке 15 ноября 2000 г. // Собрание законодательства Российской Федерации. – 2004. – № 40. – Ст. 3882. – Текст : непосредственный.

8. *Конвенция Африканского союза о кибербезопасности и защите персональных данных* 2014 г. – URL: <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>. – Текст : электронный.

9. *Резолюция* Генеральной Ассамблеи Организации Объединенных Наций от 4 января 1999 г. 53/70 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» // Официальный сайт ООН. – URL: <https://www.un.org/disarmament/ru/>. – Текст : электронный.

10. *Резолюция* Генеральной Ассамблеи Организации Объединенных Наций от 5 декабря 2018 г. 73/27 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» // Официальный сайт ООН. – URL: <https://www.un.org/disarmament/ru/>. – Текст : электронный.

11. *Резолюция* Генеральной Ассамблеи Организации Объединенных Наций от 22 декабря 2018 г. 73/264 «Поощрение ответственного поведения государств в киберпространстве в контексте международной безопасности» // Официальный сайт ООН. – URL: <https://www.un.org/disarmament/ru/>. – Текст : электронный.

12. *Резолюция* Генеральной Ассамблеи Организации Объединенных Наций от 20 декабря 2002 г. 57/239 «Элементы для создания глобальной культуры кибербезопасности» // Официальный сайт ООН. – URL: https://www.un.org/ru/documents/decl_conv/conventions/. – Текст : электронный.

13. *Факультативный протокол к Конвенции Организации Объединенных Наций о правах ребенка, касающийся торговли детьми, детской проституции и детской порнографии* : принят Генеральной Ассамблеей ООН 25 мая 2000 г. // Официальный сайт ООН. – URL: <https://www.un.org/disarmament/ru/>. – Текст : электронный.

14. *Модельный информационный кодекс для государств – участников Содружества Независимых Государств* : принят в г. Санкт-Петербурге 23 ноября 2012 г. постановлением № 38-6 на 38-м пленарном заседании Межпарламентской Ассамблеи государств – участников Содружества Независимых Государств // Информационный бюллетень Межпарламентской Ассамблеи государств –

участников Содружества Независимых Государств. – 2013. – № 57, ч. 1. – Текст : непосредственный.

15. *Соглашение о сотрудничестве государств – участников Содружества Независимых Государств с преступлениями в сфере компьютерной информации* (Минск, 1 июня 2001 г.) // Собрание законодательства Российской Федерации. – 2009. – № 13. – Ст. 1460. – Текст : непосредственный.

16. *Постановление Межпарламентской Ассамблеи государств – участников Содружества Независимых Государств от 23 ноября 2012 г. № 38-20 // Информационный бюллетень Межпарламентской Ассамблеи Содружества Независимых Государств.* – 2013. – № 57, ч. 1. – Текст : непосредственный.

17. *Постановление № 39-25 Межпарламентской Ассамблеи государств – участников Содружества Независимых Государств «Рекомендации по правовому регулированию эксплуатации открытых телекоммуникационных сетей для предупреждения их использования в террористических и иных противоправных целях»* : принято в г. Санкт-Петербурге 29 ноября 2013 г. // Информационный бюллетень Межпарламентской Ассамблеи государств – участников Содружества Независимых Государств. – 2013. – № 57, ч. 2. – Текст : непосредственный.

18. *Постановление № 41-14 Межпарламентской Ассамблеи государств – участников Содружества Независимых Государств «О модельном законе „О критически важных объектах информационно-коммуникационной инфраструктуры“»* : принято в г. Санкт-Петербурге 28 ноября 2014 г. // Информационный бюллетень Межпарламентской Ассамблеи государств – участников Содружества Независимых Государств. – 2015. – № 62, ч. 2. – Текст : непосредственный.

19. *Постановление № 41-17 Межпарламентской Ассамблеи государств – участников Содружества Независимых Государств «О модельном Регламенте административных процедур, осуществляемых уполномоченными органами в сфере обеспечения информационной безопасности государств – участников Содружества Независимых Государств»* : принято в г. Санкт-Петербурге 28 ноября

2014 г. // Информационный бюллетень Межпарламентской Ассамблеи государств – участников Содружества Независимых Государств. – 2014. – № 57, ч. 2. – Текст : непосредственный.

20. *Постановление* № 40-12 Межпарламентской Ассамблеи государств – участников Содружества Независимых Государств «О Рекомендациях по совершенствованию законодательства о выборах глав государств в странах Содружества Независимых Государств : принято в г. Санкт-Петербурге 18 апреля 2014 г. // Информационный бюллетень Межпарламентской Ассамблеи государств – участников Содружества Независимых Государств. – 2014. – № 61. – Текст : непосредственный.

21. *Федеральный закон* от 7 мая 2013 г. № 76-ФЗ «О ратификации Конвенции Совета Европы о защите детей от сексуальной эксплуатации и сексуальных злоупотреблений». – Доступ из справ.-правовой системы «КонсультантПлюс». – Текст : электронный.

22. *Федеральный закон* от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». – Доступ из справ.-правовой системы «КонсультантПлюс». – Текст : электронный.

23. *Закон Республики Казахстан* от 16 ноября 2015 г. № 401-V ЗРК «О доступе к информации» // Казахстанская правда. – 2015. – 19 нояб. – Текст : непосредственный.

24. *Закон Республики Казахстан* от 29 апреля 2010 г. № 271-IV «О профилактике правонарушений». – URL: <https://adilet.zan.kz/rus>. – Текст : электронный.

25. *Федеральный закон* от 27 июля 2006 г. № 152-ФЗ «О персональных данных». – Доступ из справ.-правовой системы «КонсультантПлюс». – Текст : электронный.

26. *Федеральный закон* от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию». – Доступ из справ.-правовой системы «КонсультантПлюс». – Текст : электронный.

27. *Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».* – Доступ из справ.-правовой системы «КонсультантПлюс». – Текст : электронный.

28. *Федеральный закон от 2 июля 2013 г. № 187-ФЗ «О внесении изменений в законодательные акты Российской Федерации по вопросам защиты интеллектуальных прав в информационно-телекоммуникационных сетях».* – Доступ из справ.-правовой системы «КонсультантПлюс». – Текст : электронный.

29. *Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».* – Доступ из справ.-правовой системы «КонсультантПлюс». – Текст : электронный.

30. *Федеральный закон от 23 апреля 2018 г. № 111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации».* – Доступ из справ.-правовой системы «КонсультантПлюс». – Текст : электронный.

31. *Федеральный закон от 31 июля 2020 г. № 259-ФЗ «О финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации».* – Доступ из справ.-правовой системы «КонсультантПлюс». – Текст : электронный.

32. *Указ Президента Российской Федерации от 12 декабря 2014 г. № К-1274 «Об утверждении концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».* – Доступ из справ.-правовой системы «Гарант». – Текст : электронный.

33. *Указ Президента Российской Федерации от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года»)».* – Доступ из справ.-правовой системы «Гарант». – Текст : электронный.

34. *Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» //*

Собрание законодательства Российской Федерации. – 2016. – № 50. – Ст. 7074. – Текст : непосредственный.

35. *Указ* Президента Российской Федерации от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // Собрание законодательства Российской Федерации. – 2017. – № 20. – Ст. 2901. – Текст : непосредственный.

36. *Указ* Президента Российской Федерации от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации». – Доступ из справ.-правовой системы «КонсультантПлюс». – Текст : электронный.

37. *Указ* Президента Российской Федерации от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации». – Доступ из справ.-правовой системы «КонсультантПлюс». – Текст : электронный.

38. *Распоряжение* Правительства Российской Федерации от 19 августа 2020 г. «Об утверждении концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 г.». – Доступ из справ.-правовой системы «КонсультантПлюс». – Текст : электронный.

39. *Постановление* Правительства Республики Казахстан от 8 сентября 2016 г. № 529 «Об утверждении Правил и критериев отнесения объектов информационно-коммуникационной инфраструктуры к критически важным объектам информационно-коммуникационной инфраструктуры» // Казахстанская правда. – 2016. – 17 сент. – Текст : непосредственный.

40. *Постановление* Правительства Республики Казахстан от 30 декабря 2021 г. № 961 «Об утверждении Концепции развития отрасли информационно-коммуникационных технологий и цифровой сферы». – URL: <https://adilet.zan.kz/>. – Текст : электронный.

41. *Постановление* Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // Собрание законодательства Российской Федерации. – 2012. – № 45. – Ст. 6257. – Текст : непосредственный.

42. *Постановление* Правительства Российской Федерации от 15 апреля 2014 г. № 313 «Об утверждении государственной программы Российской Федерации „Информационное общество (2011–2020 годы)“». – Доступ из справ.-правовой системы «КонсультантПлюс». – Текст : электронный.

43. *Постановление* Правительства Республики Казахстан от 30 июня 2017 г. № 407 «Об утверждении Концепции кибербезопасности («Киберцит Казахстана»)). – URL: <https://adilet.zan.kz/rus/docs/>. – Текст : электронный.

44. *Распоряжение* Правительства Российской Федерации от 28 июля 2017 г. № 1632-р «Об утверждении программы „Цифровая экономика Российской Федерации“» // Собрание законодательства Российской Федерации. – 2017. – № 32. – Ст. 5138. – Текст : непосредственный.

45. *Распоряжение* Правительства Российской Федерации от 16 июля 2009 г. № 984-р «Об утверждении Соглашения между правительствами государств – членов Шанхайской организации о сотрудничестве в области обеспечения международной информационной безопасности» // Собрание законодательства Российской Федерации. – 2009. – № 30 – Ст. 3879. – Текст : непосредственный.

46. *Стратегия* развития информационного общества в Российской Федерации на 2017–2030 гг. // Собрание законодательства Российской Федерации. – 2017. – № 20. – Ст. 2901. – Текст : непосредственный.

47. *Постановление* Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате». – Доступ из справ.-правовой системы «КонсультантПлюс». – Текст : электронный.

48. *Постановление* Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть „Интернет“». – Доступ из справ.-правовой системы «КонсультантПлюс». – Текст : электронный.

49. *Приказ* МВД России, Минюста России, ФСБ России, ФСО России, ФСКН России, ФТС России от 6 октября 2006 г. № 786/310/470/454/333/971 «Об утверждении Инструкции по организации информационного обеспечения сотрудничества по линии Интерпола» // Бюллетень нормативных актов федеральных органов исполнительной власти. – 2006. – № 47. – Текст : непосредственный.

50. *Приказ* МВД России от 3 февраля 2012 г. № 77 «Об основах организации ведомственного контроля за деятельностью органов внутренних дел Российской Федерации». – Доступ из справ.-правовой системы «КонсультантПлюс». – Текст : электронный.

51. *Приказ* МВД России от 1 декабря 2016 г. № 777 «Об организации постоянного мониторинга общественного мнения о деятельности полиции». – Доступ из справ.-правовой системы «КонсультантПлюс». – Текст : электронный.

52. *Приказ* МВД России от 27 декабря 2018 г. № 886 «Об утверждении положения о взаимодействии при осуществлении деятельности по предупреждению, выявлению, пресечению и раскрытию правонарушений, связанных с незаконным оборотом наркотических средств, психотропных веществ и их прекурсоров, сильнодействующих или ядовитых веществ». – Доступ из справ.-правовой системы «КонсультантПлюс». – Текст : электронный.

53. *Приказ* МВД России от 15 июня 2021 г. № 444 «Об утверждении Положения о Департаменте информационных технологий, связи и защиты информации Министерства внутренних дел Российской Федерации». – Доступ из справ.-правовой системы «КонсультантПлюс». – Текст : электронный.

54. *Приказ* МВД России от 24 августа 2023 г. № 619 «О некоторых организационных вопросах деятельности органов внутренних дел Российской Федерации по профилактике правонарушений» – Доступ из справ.-правовой системы «КонсультантПлюс». – Текст : электронный.

55. *Приказ* ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных

системах персональных данных» // Российская газета. – 2013. – 22 мая. – Текст : непосредственный.

56. *Приказ* Главного управления МВД России по г. Москве от 27 апреля 2022 г. № 143 «Об организации эксплуатации сервисов ИСОД МВД России» // Официальный сайт Министерства внутренних дел Российской Федерации. – URL: <https://77.мвд.рф/documents/приказы-гу-мвд-россии-по-г.москве/item/30183603/>. – Текст : электронный.

57. *Письмо* Генпрокуратуры России от 19 сентября 2023 г. № 36-49-2023 «О методических рекомендациях по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации». – Доступ из справ.-правовой системы «КонсультантПлюс». – Текст : электронный.

58. *Распоряжение* МВД России от 10 апреля 2020 г. № 1/4005 «Об утверждении плана информатизации МВД России на 2020 год и плановый период 2021 и 2022 годов (открытая часть)». – Доступ из справ.-правовой системы «Консультант Плюс». – Текст : электронный.

Материалы судебной практики

59. *Отчет* о демографических признаках осужденных по всем составам преступлений УК РФ. – URL: http://www.cdep.ru/userimages/sudebnaya_statistika/2022/k5_1-svod_vse_sudy-2022.xls. – Текст : электронный.

60. *Постановление* Южно-Сахалинского городского суда Сахалинской области по уголовному делу от 15 августа 2019 г. № 1-908/2019 // Судебные и нормативные акты РФ. – URL: www.sudact.ru/regular/doc/6ywo62uBMgoC. – Текст : электронный.

61. *Постановление* Ангарского городского суда Иркутской области по уголовному делу от 29 ноября 2019 г. № 1-1410/2019 // Судебные и нормативные акты РФ. – URL: www.sudact.ru/regular/doc/GLwzW3qei9rm. – Текст : электронный.

62. *Постановление* Комсомольского районного суда г. Тольятти Самарской области по уголовному делу от 9 декабря 2019 г. № 1-269/2019 // Судебные и нормативные акты РФ. – URL: www.sudact.ru/regular/doc. – Текст : электронный.

63. *Приговор* Казыбекбийского районного суда г. Караганды в отношении гр. О. от 15 сентября 2016 г. № 3511-16-00-1/390/2016 // Банк судебных актов. – URL: <https://office.sud.kz/>. – Текст : электронный.

64. *Приговор* Казыбекбийского районного суда города Караганды в отношении гр. А. от 7 октября 2016 г. № 3511-16-00-1/299 // Банк судебных актов. – URL: <https://office.sud.kz/>. – Текст : электронный.

65. *Приговор* Алатауского районного суда города Алматы в отношении гр. М. от 17 ноября 2016 г. № 1-397/2016 // Банк судебных актов. – URL: <https://office.sud.kz/>. – Текст : электронный.

66. *Приговор* по уголовному делу районного суда № 2 Бостандыкского района г. Алматы от 24 января 2017 г. №157500121001309 // Банк судебных актов. – URL: <https://office.sud.kz/>. – Текст : электронный.

67. *Приговор* Рудничного районного суда г. Кемерово Кемеровской области от 31 января 2017 г. № 1-41/2017 // Судебные и нормативные акты РФ. – URL: <https://sudact.ru>. – Текст : электронный.

68. *Приговор* Советского районного суда г. Казани Республики Татарстан от 15 марта 2017 г. № 1-81/2017 // Судебные и нормативные акты РФ. – URL: <https://sudact.ru>. – Текст : электронный.

69. *Приговор* Ленинского районного суда г. Ульяновска от 14 апреля 2017 г. № 1-37/2017 // Судебные и нормативные акты РФ. – URL: <https://sudact.ru>. – Текст : электронный.

70. *Приговор* Алатауского районного суда города Алматы в отношении гр. К. от 26 апреля 2017 г. № 1-175/2017 // Банк судебных актов. – URL: <https://office.sud.kz/>. – Текст : электронный.

71. *Приговор* районного суда № 2 Бостандыкского района города Алматы в отношении гр. Х. от 10 мая 2017 г. № 7550-17-00-1/123 // Банк судебных актов. – URL: <https://office.sud.kz/>. – Текст : электронный.

72. *Приговор* Советского районного суда г. Уфы от 4 августа 2017 г. № 1-397/2017 // Судебные и нормативные акты РФ. – URL: <https://sudact.ru>. – Текст : электронный.

73. *Приговор* Алатауского районного суда города Алматы в отношении гр. Ч. от 18 августа 2017 г. № 1-319/2017 // Банк судебных актов. – URL: <https://office.sud.kz/>. – Текст : электронный.

74. *Приговор* Октябрьского районного суда г. Самары от 18 сентября 2017 г. по делу № 1-192/2017 // Судебные и нормативные акты РФ. – URL: <https://sudact.ru/regular>. – Текст : электронный.

75. *Приговор* Промышленного районного суда г. Оренбурга от 16 октября 2017 г. № 1-392/2017 // Судебные и нормативные акты РФ. – URL: <https://sudact.ru>. – Текст : электронный.

76. *Приговор* Заельцовского районного суда г. Новосибирска Новосибирской области по уголовному делу от 13 ноября 2017 г. № 1-158/2017 // Судебные и нормативные акты РФ. – URL: www.sudact.ru/regular. – Текст : электронный.

77. *Приговор* Советского районного суда г. Воронежа от 28 ноября 2017 г. № 1-381/2017 // Судебные и нормативные акты РФ. – URL: <https://sudact.ru>. – Текст : электронный.

78. *Приговор* районного суда № 2 Жетысуского района города Алматы в отношении гр. К. от 9 января 2018 г. № 7560-17-00-1/664 // Банк судебных актов. – URL: <https://office.sud.kz/>. – Текст : электронный.

79. *Приговор* Созакского районного суда Южно-Казахстанской области в отношении гр. У. от 29 марта 2018 г. № 5156-18-00-1/10 // Банк судебных актов. – URL: <https://office.sud.kz/>. – Текст : электронный.

80. *Приговор* Кировского районного суда г. Хабаровска от 11 декабря 2018 г. по ч. 2 ст. 272 УК РФ № 1-3/2017 (№ 1-45/2016) // Судебная практика РФ. – URL: sud-praktika.ru. – Текст : электронный.

81. *Приговор* Сыктывкарского городского суда Республики Коми по уголовному делу от 22 ноября 2018 г. № 1-710/2018 // Судебные и нормативные акты РФ. – URL: www.sudact.ru/regular/doc/t3IB9ntfbkQC. – Текст : электронный.

82. *Приговор* районного суда № 2 Бостандыкского района г. Алматы в отношении гр. Л. от 7 февраля 2019 г. № 7550-18-00-1\544 // Банк судебных актов. – URL: <https://office.sud.kz/>. – Текст : электронный.

83. *Приговор* Бугурусланского районного суда Оренбургской области по уголовному делу от 18 июля 2019 г. № 1-149/2019 // Судебные и нормативные акты РФ. – URL: www.sudact.ru/regular/doc. – Текст : электронный.

84. *Приговор* Кирсановского районного суда Тамбовской области по уголовному делу от 28 августа 2019 г. № 1-140/2019 // Судебные и нормативные акты РФ. – URL: www.sudact.ru/regular/doc/NoCBWztR5OdC. – Текст : электронный.

85. *Приговор* Кировского районного суда г. Ростова-на-Дону Ростовской области по уголовному делу от 13 сентября 2019 г. № 1-345/2019 // Судебные и нормативные акты РФ. – URL: www.sudact.ru/regular/doc. – Текст : электронный.

86. *Приговор* суда № 2 Есильского района города Нур-Султан в отношении гр. К. и С. от 10 февраля 2020 г. № 7135-19-00-1/367 // Банк судебных актов. – URL: <https://office.sud.kz/>. – Текст : электронный.

87. *Приговор* Сормовского районного суда г. Нижний Новгород от 29 апреля 2020 г. по делу № 1-211/2020 // Судебные и нормативные акты РФ. – URL: <https://sudact.ru>. – Текст : электронный.

88. *Приговор* суда № 2 г. Усть-Каменогорска Восточно-Казахстанской области в отношении гр. К. и Л. от 14 августа 2020 г. № 1-189 // Банк судебных актов. – URL: <https://office.sud.kz/>. – Текст : электронный.

89. *Приговор* Калининского районного суда г. Санкт-Петербурга от 4 сентября 2020 г. № 1-626/2020 // Судебные и нормативные акты РФ. – URL: <https://sudact.ru>. – Текст : электронный.

90. *Приговор* Павловского районного суда Воронежской области от 25 ноября 2020 г. № 1-40/2020 // Судебные и нормативные акты РФ. – URL: <https://sudact.ru>. – Текст : электронный.

91. *Приговор* Киевского районного суда города Симферополя Республики Крым от 29 июня 2021 г. № 1-272/2021 // Судебные и нормативные акты РФ. – URL: <https://sudact.ru>. – Текст : электронный.

92. *Приговор* Чусовского городского суда Пермского края от 7 июля 2021 г. № 1-175/2021 // Судебные и нормативные акты РФ. – URL: <https://sudact.ru>. – Текст : электронный.

93. *Приговор* Ангарского городского суда Иркутской области от 21 июля 2021 г. № 1-763/2021 // Судебные и нормативные акты РФ. – URL: <https://sudact.ru>. – Текст : электронный.

94. *Приговор* Шадринского районного суда Курганской области от 28 июля 2021 г. № 1-281/2021 // Судебные и нормативные акты РФ. – URL: <https://sudact.ru>. – Текст : электронный.

95. *Приговор* районного суда № 2 Бостандыкского района г. Алматы РК от 16 августа 2021 г. № 7550-21-00-1/243 в отношении О. // Банк судебных актов. – URL: <https://sud.gov.kz/rus/bank>. – Текст : электронный.

96. *Приговор* Ленинского районного суда г. Пензы от 20 сентября 2021 г. № 1-234/2021 // Судебные и нормативные акты РФ. – URL: <https://sudact.ru>. – Текст : электронный.

97. *Приговор* Алмалинского районного суда города Алматы в отношении гр. Г. и К. от 21 декабря 2021 г. № 1-548/21 // Банк судебных актов. – URL: <https://office.sud.kz/>. – Текст : электронный.

98. *Приговор* Медеуского районного суда города Алматы в отношении гр. М. от 4 октября 2021 г. № 7525-21-00-1/268 // Банк судебных актов. – URL: <https://office.sud.kz/>. – Текст : электронный.

99. *Приговор* Казыбекбийского районного суда города Караганды в отношении гр. К. от 3 февраля 2022 г. № 3511-21-00-1 // Банк судебных актов. – URL: <https://office.sud.kz/>. – Текст : электронный.

100. *Приговор* Преображенского районного суда г. Москвы от 14 апреля 2022 г. № 1-363/22 // Судебные и нормативные акты РФ. – URL: <https://sudact.ru>. – Текст : электронный.

101. *Приговор* суда № 2 города Тараз в отношении гр. Т. от 30 ноября 2022 г. № 3111-22-00-1/592 // Банк судебных актов. – URL: <https://office.sud.kz/>. – Текст : электронный.

102. *Приговор* Хромтауского районного суда Актюбинской области от 5 января 2023 г. № 1560-22-00-1/81 // Банк судебных актов. – URL: <https://office.sud.kz/>. – Текст : электронный.

103. *Приговор* Риддерского городского суда Восточно-Казахстанской области в отношении гр. К. от 22 февраля 2023 г. № 6324-23-00-1/18 // Банк судебных актов. – URL: <https://office.sud.kz/>. – Текст : электронный.

104. *Приговор* Кордайского районного суда Жамбылской области в отношении гр. М. от 3 марта 2023 г. № 3148-23-00-1/17 // Банк судебных актов. – URL: <https://office.sud.kz/>. – Текст : электронный.

105. *Приговор* Кокшетауского городского суда Акмолинской области в отношении гр. Ч. от 21 апреля 2023 г. № 1110-23-00-1/62 // Банк судебных актов. – URL: <https://office.sud.kz/>. – Текст : электронный.

106. *Приговор* суда района Беимбета Майлина Костанайской области в отношении гр. Т. от 15 мая 2023 г. № 3964-23-00-1/18 // Банк судебных актов. – URL: <https://office.sud.kz/>. – Текст : электронный.

107. *Приговор* суда № 2 г. Актюбинска Актюбинской области в отношении гр. К. от 15 мая 2023 г. № 1511-23-00-1/174 // Банк судебных актов. – URL: <https://office.sud.kz/>. – Текст : электронный.

108. *Приговор* Абайского районного суда Карагандинской области в отношении гр. Б. от 29 мая 2023 г. № 3532-23-00-1/34 // Банк судебных актов. – URL: <https://office.sud.kz/>. – Текст : электронный.

109. *Приговор* Перовского районного суда г. Москвы от 28 июня 2023 г. № 1-689/2023 // Судебные и нормативные акты РФ. – URL: <https://sudact.ru>. – Текст : электронный.

110. *Приговор* суда Байганинского района Актюбинской области в отношении гр. К. от 10 ноября 2023 г. № 1536-23-00-1/21а // Банк судебных актов. – URL: <https://office.sud.kz/>. – Текст : электронный.

111. *Приговор* суда № 2 г. Усть-Каменогорска Восточно-Казахстанской области в отношении гр. Р. и Т. от 16 января 2024 г. № 1-493/2023 г. // Банк судебных актов. – URL: <https://office.sud.kz/>. – Текст : электронный.

Научная и учебная литература

112. *Алауханов, Е. О.* Криминология : учебник / Е. О. Алауханов. – Санкт-Петербург : Юридический Центр Пресс, 2013. – 824 с. – Текст : непосредственный.

113. *Антонян, Ю. М.* Криминология. Избранные лекции / Ю. М. Антонян. – Москва : Лотос, 2004. – 448 с. – Текст : непосредственный.

114. *Вицин, С. Е.* Системный подход и преступность : учебное пособие / С. Е. Вицин. – Москва : Академия МВД СССР, 1980. – 140 с. – Текст : непосредственный.

115. *Джафарли, В. Ф.* Криминология кибербезопасности : в 5 т. – Т. 1 : Криминологическая кибербезопасность: теоретические, правовые и технологические основы / В. Ф. Джафарли. – Москва : Проспект, 2021. – 288 с. – Текст : непосредственный.

116. *Джекебаев, У. С.* Преступность как криминологическая проблема / У. С. Джекебаев. – Алма-Ата : Наука, 1974. – 128 с. – Текст : непосредственный.

117. *Исмагулова, А. Т.* Уголовные правонарушения в сфере информатизации и связи в Республике Казахстан : монография / А. Т. Исмагулова, А. М. Галиаскарова. – Костанай : ТОО «Neo Line Media», 2016. – 160 с. – Текст : непосредственный.

118. *Киберпреступность.* Модуль 1. Введение в киберпреступность. – Вена, 2019. – 36 с. – Текст : непосредственный.

119. *Клеймёнов, М. П.* Криминология : учебник / М. П. Клеймёнов. – Москва : Норма, 2009. – 448 с. – Текст : непосредственный.

120. *Колчевский, И. Б.* Новые способы совершения преступлений в сфере информационных технологий на территории государств – участников СНГ : аналитический обзор / И. Б. Колчевский, В. М. Журавлев, А. Г. Кузнецов и О. В. Демковец, Д. А. Брехов. – Москва : ФГКУ «ВНИИ МВД России», 2018. – 76 с. – Текст : непосредственный.

121. *Криминология* : учебник / Г. А. Аванесов, С. М. Иншаков, Е. А. Антонян ; под ред. Г. А. Аванесова. – 7-е изд., перераб и доп. – Москва : ЮНИТИ, ЮНИТИ ДАНА, 2020. – 448 с. – Текст : непосредственный.

122. *Криминология* : учебник для вузов / под общ. ред. д-ра юрид. наук, проф. А. И. Долговой. – 3-е изд., перераб. и доп. – Москва : Норма, 2005. – 912 с. – Текст : непосредственный.

123. *Криминология* : учебник / под ред. В. Д. Малкова. – Москва : Юридический Дом «Юстицинформ», 2004. – 524 с. – Текст : непосредственный.

124. *Криминология. Общая часть.* : учебник для вузов / М. А. Кириллов [и др.] ; под общ. ред. д-ра юрид. наук, проф. М. А. Кириллова, д-ра юрид. наук, проф. В. И. Омигова. – Чебоксары : ЧКИ РУК, 2010. – 257 с. – Текст : непосредственный.

125. *Каиржанов, Е. И.* Криминология : учебник для вузов. Общая часть / Е. И. Каиржанов. – Алматы : Оркениет, 2000. – 288 с. – Текст : непосредственный.

126. *Кузнецова, Н. Ф.* Криминология : учебник / Н. Ф. Кузнецова, В. В. Лунеев. – 2-е изд., перераб. и доп. – Москва : Волтерс Клувер, 2004. – 629 с. – Текст : непосредственный.

127. *Мацкевич, И. М.* Криминология : учебник для аспирантов / И. М. Мацкевич. – Москва : Норма, 2017. – 368 с. – Текст : непосредственный.

128. *Научно-практический комментарий* Федерального закона Российской Федерации от 23 июня 2016 года № 182-ФЗ «Об основах системы профилактики правонарушений в Российской Федерации» / под общ. ред. д-ра юрид. наук, профессора В. И. Майорова. – Тюмень: Тюменский институт повышения квалификации сотрудников МВД России, 2017. – 84 с. – Текст : непосредственный.

129. *Осипенко, А. Л.* Сетевая компьютерная преступность: теория и практика борьбы : монография / А. Л. Осипенко. – Омск : Омская академия МВД России, 2009. – 480 с. – Текст : непосредственный.

130. *Основы криминологии* : учебник / под ред. А. Ф. Федорова, С. Я. Лебедева. – 2-е изд. – Москва : Юнити-Дана. – 415 с. – Текст : непосредственный.

131. *Преступления, совершаемые с использованием информационных технологий: проблемы квалификации и особенности расследования* : монография / А. Ф. Абдулвалиев, А. В. Белоусов, Ж. В. Вассалатий [и др.] ; под науч. ред. проф. Е. В. Смахтина, проф. Р. Д. Шарапова, доц. В. И. Морозова. – Тюмень : Издательство Тюменского государственного университета, 2021. – Текст : электронный.

132. *Рассолов, И. М. Право и Интернет. Теоретические проблемы* / И. М. Рассолов. – Москва : Норма, 2003. – 331 с. – Текст : непосредственный.

133. *Семь безопасных информационных технологий* / А. С. Марков, А. В. Дорофеев, А. В. Барабанов, В. А. Цирлов. – Москва : ДМК-Пресс, 2017. – 224 с. – Текст : непосредственный.

134. *Современное состояние и тенденции развития киберпреступности на пространстве Содружества Независимых Государств : аналитический обзор с предложениями* / Н. Н. Дьяченко, О. А. Надейкина, Д. В. Кирган, И. А. Грозан, В. А. Казакова, О. И. Новосельцев, О. В. Демковец. – Москва : ВНИИ МВД России, 2023. – 72 с. – Текст : непосредственный.

135. *Стручков, Н. А. Преступность как социальное явление* / Н. А. Стручков. – Ленинград : Б. и., 1979. – 120 с. – Текст : непосредственный.

136. *Ушатиков, А. И. Прикладная криминальная психология : учебное пособие* / А. И. Ушатиков, О. Г. Ковалев, Г. К. Корнеева. – Рязань, 2012. – 596 с. – Текст : непосредственный.

137. *Федоров, А. В. Информационная безопасность в мировом политическом процессе : учебное пособие* / А. В. Федоров. – Москва : МГИМО–Университет, 2006. – 220 с. – Текст : непосредственный.

138. *Шестаков, Д. А. Криминология: Преступность как свойство общества : краткий курс* / Д. А. Шестаков. – Санкт-Петербург : Лань, 2001. – 259 с. – Текст : непосредственный.

Научные статьи и публикации

139. *Айсханова, Е. С.* Причины и мотивы роста киберпреступности как глобального явления современности / Е. С. Айсханова. – Текст : непосредственный // Вестник Чеченского государственного университета. – 2017. – № 4. – С. 153–155.

140. *Аккузин, Ю. А.* Кибернетические преступления как новая угроза обществу / Ю. А. Аккузин, В. В. Леонов. – Текст : непосредственный // Закон и право. – 2020. – № 4. – С. 197–200.

141. *Бабурин, В. В.* 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(96). – С. 95–100.

142. *Бабурин, В. В.* Детерминанты киберпреступлений, совершаемых в сфере экономики / В. В. Бабурин. – Текст : непосредственный // Преступность в сфере экономики: современные тенденции и проблемы противодействия : мат-лы междунар. науч.-практ. конф. – Омск : Омская академия МВД России, 2023. – С. 3–6.

143. *Бабурин, В. В.* Теория причин преступности в российской криминологии: проблемы становления и перспективы развития / В. В. Бабурин, П. Л. Сурихин. – Текст : непосредственный // Вестник Уральского юридического института МВД России. – 2023. – № 4. – С. 138–143.

144. *Байрамов, Р. Р.* Анализ киберпреступлений и мер по их предупреждению / Р. Р. Байрамов, В. А. Пасат. – Текст : непосредственный // Ученые записки Санкт-Петербургского имени В. Б. Бобкова филиала Российской таможенной академии. – 2022. – № 1(81). – С. 63–67.

145. *Бегишев, И. Р.* Организация хакерского сообщества: криминологический и уголовно-правовой аспекты / И. Р. Бегишев, З. И. Хисамова, С. Г. Никитин. – Текст : непосредственный // Всероссийский криминологический журнал. – 2020. – Т. 14, № 1. – С. 96–105.

146. *Бегишев, И. Р.* Регулирование технологий искусственного интеллекта: столкновение этики и закона / И. Р. Бегишев, А. А. Шутова. – Текст : непосредственный // Лоббирование в законодательстве. – 2025. – Т. 4, № 1. – С. 21–28.

147. *Бегишев, И. Р.* Культура информационной безопасности: психолого-правовой аспект / И. Р. Бегишев. – Текст : непосредственный // Психология и право. – 2021. – Т. 11, № 4. – С. 207–220.

148. *Белевитина, Ю. В.* Криминологический портрет личности киберпреступника в современной России / Ю. В. Белевитина. – Текст : непосредственный // Инновационная наука. – 2022. – № 12-2. – С. 61–64.

149. *Бородкина, Т. Н.* Киберпреступления: понятие, содержание и меры противодействия / Т. Н. Бородкина, А. В. Павлюк. – Текст : непосредственный // Социально-политические науки. – 2018. – № 1. – С. 135–137.

150. *Глотина, И. М.* Киберпреступность как теневой бизнес / И. М. Глотина. – Текст : непосредственный // Вестник Челябинского государственного университета. – 2016. – № 6. – С. 51–57.

151. *Григор, А. А.* Понятия «профилактика» и «предупреждение» преступности в контексте исследования российского законодательства / А. А. Григор. – Текст : непосредственный // Проблемы социально-гуманитарного образования на современном этапе модернизации российской школы: мат-лы девятой всерос. с междунар. участием науч.-практ. конф. – Барнаул : Алтай. гос. пед. ун-т, 2021. – С. 130–133.

152. *Григорян, С. А.* Особенности личности современного «киберпреступника» / С. А. Григорян. – Текст : непосредственный // Наука и образование: хозяйство и экономика; предпринимательство; право и управление. – 2022. – № 8(147). – С. 103–106.

153. *Гундериц, Г. А.* Состояние киберпреступности / Г. А. Гундериц. – Текст : непосредственный // Научный вестник Крыма. – 2018. – № 4. – С. 11–19.

154. *Джансараева, Р. Е.* Борьба с киберпреступлениями: сравнительный анализ законодательства стран СНГ / Р. Е. Джансараева, К. Аратулы. – Текст :

непосредственный // Криминологический журнал Байкальского государственного университета экономики и права. – 2012. – № 3. – С. 95–99.

155. *Джафарли, В. Ф.* Краткий криминологический анализ причин и условий киберпреступности и методы ее предупреждения / В. Ф. Джафарли. – Текст : непосредственный // Ученые труды Российской академии адвокатуры и нотариата. – 2017. – № 2(45). – С. 54–58.

156. *Долгополов, А. А.* Об уголовно-правовых и криминологических аспектах личности преступника и преступного поведения / А. А. Долгополов, А. Н. Ильяшенко, А. В. Белоконь. – Текст : непосредственный // Вестник Казанского юридического института МВД России. – 2024. – № 3. – С. 47–54.

157. *Дыбыс, Р. Т.* Административно-правовые средства обеспечения информационной безопасности в Республике Казахстан / Р. Т. Дыбыс. – Текст : непосредственный // Казахская цивилизация. – 2017. – № 3. – С. 47–54.

158. *Евдокимов, К. Н.* Актуальные вопросы предупреждения киберпреступности в Российской Федерации / К. Н. Евдокимов. – Текст : непосредственный // Актуальные проблемы борьбы с преступностью: вопросы теории и практики : мат-лы XV междунар. науч.-практ. конф. – Красноярск, 2022. – Ч. 2. – С. 58–59.

159. *Евдокимов, К. Н.* Актуальные вопросы противодействия компьютерной преступности в Российской Федерации (криминологическое исследование) / К. Н. Евдокимов. – Текст : непосредственный // Российский следователь. – 2018. – № 10. – С. 56–61.

160. *Евдокимов, К. Н.* Анекселенктотичная технотронная преступность (частная теория) / К. Н. Евдокимов. – Текст : непосредственный // Российский судья. – 2018. – № 4. – С. 35–39.

161. *Евдокимов, К. Н.* Причины компьютерной преступности в современной России / К. Н. Евдокимов. – Текст : непосредственный // Российский следователь. – 2015. – № 3. – С. 33–37.

162. *Журавленко, Н. И.* Проблемы борьбы с киберпреступностью и перспективные направления международного сотрудничества в этой сфере /

Н. И. Журавленко, Л. Е. Шведова. – Текст : непосредственный // Общество и право. – 2015. – № 3(53). – С. 66–70.

163. *Иванов, Н. Н.* Интенсификация информационного обеспечения управления: проблемы и пути решения / Н. Н. Иванов. – Текст : непосредственный // Интенсификация информационного обеспечения управления в органах внутренних дел : тр. Академии МВД России. – Москва : Академия МВД России, 1992. – С. 3–10.

164. *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.

165. *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.

166. *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.

167. *Карабеков, К. О.* Криминологическая характеристика личности киберпреступника в Российской Федерации и Республике Казахстан / К. О. Карабеков, В. В. Бабурин. – Текст : непосредственный // Психопедагогика в правоохранительных органах. – 2024. – № 1(96). – С. 113–119.

168. *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 : мат-лы XX междунар. науч.-практ. конф. : в 2 ч. – Барнаул : Барнаульский юридический институт МВД России, 2022. – Ч. 2. – С. 25–27.

169. *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 : мат-лы междунар. науч.-практ. семинара. – Красноярск : Сибирский юридический институт МВД России, 2022. – С. 96–99.

170. *Карабеков, К. О.* Роль кибердружин в противодействии интернет-угрозам / К. О. Карабеков. – Текст : непосредственный // Современные тенденции развития юридической науки : мат-лы междунар. науч.-теор. конф. молодых ученых, посвященной Дню казахстанской науки. – Караганда : Карагандинская академия имени Баримбека Бейсенова, 2022. – С. 36–38.

171. *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 : мат-лы междунар. науч.-практ. конф., посвященной 30-летию казахстанской полиции. – Караганда : Карагандинская академия имени Баримбека Бейсенова, 2022. – С. 98–102.

172. *Карабеков, К. О.* Профилактика кибербуллинга в подростковой среде / К. О. Карабеков. – Текст : непосредственный // Защита прав детей: сотрудничество полиции и гражданского общества : мат-лы междунар. науч.-практ. конф. – Костанай : Костанайская академия имени Шракбека Кабылбаева, 2022. – С. 71–76.

173. *Карабеков, К. О.* Опыт Республики Казахстан по борьбе с киберпреступностью / К. О. Карабеков. – Текст : непосредственный // Преемственность и новации в юридической науке : мат-лы всерос. науч. конф. адъюнктов, аспирантов и соискателей. – Омск : Омская академия МВД России, 2022. – Вып. 18. – С. 58–59.

174. *Карабеков, К. О.* Причины и условия киберпреступности в Республике Казахстан / К. О. Карабеков. – Текст : непосредственный // Актуальные проблемы профилактики преступлений : мат-лы междунар. науч.-практ. семинара. – Омск : Омская академия МВД России, 2023. – С. 47–50.

175. *Карабеков, К. О.* Проблемы предупреждения киберпреступлений в Республике Казахстан / К. О. Карабеков. – Текст : непосредственный // Актуальные проблемы уголовной и уголовно-процессуальной политики Российской Федерации : мат-лы междунар. науч.-практ. конф. – Омск : Сибирский юридический университет, 2023. – С. 118–122.

176. *Карабеков, К. О.* Актуальность использования возможностей нейросетей в предупреждении преступности / К. О. Карабеков. – Текст : непосредственный // Преемственность и новации в юридической науке : мат-лы междунар. науч. конф. адъюнктов, аспирантов и соискателей. – Омск : Омская академия МВД России, 2023. – Вып. 19. – С. 50–52.

177. *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.

178. *Кецко, К. В.* Отдельные особенности личности экономического преступника, действующего в сфере электронной коммерции / К. В. Кецко. – Текст : непосредственный // Право и государство: теория и практика. – 2022. – № 7(211). – С. 135–138.

179. *Кильмаматова, Э. Р.* Международное регулирование преступлений в сфере кибертерроризма / Э. Р. Кильмаматова. – Текст : непосредственный // Современные вопросы государства, права, юридического образования : сб. науч. тр. по мат-лам XV междунар. науч.-практ. конф. – Тамбов : Издательский дом «Державинский», 2020. – С. 334–340.

180. *Клишков, В. Б.* Преступность и ее основные характеристики на современном этапе / В. Б. Клишков, В. В. Пасынков, Е. В. Стебенева. – Текст : непосредственный // Вестник Санкт-Петербургского университета МВД России. – 2015. – № 4(68). – С. 122–127.

181. *Кобец, П. Н.* Киберпреступность: современные виды, причины, ее порождающие, и особенности предупреждения / П. Н. Кобец. – Текст :

непосредственный // Вестник Самарского юридического института. – 2022. – № 1(47). – С. 52–58.

182. *Кобец, П. Н.* Правовые основы предупреждения киберпреступлений: отечественный и зарубежный опыт / П. Н. Кобец. – Текст : непосредственный // Научный вестник Омской академии МВД России. – 2022. – № 2(85). – С. 101–105.

183. *Коробеев, А. И.* Киберпреступность в Российской Федерации: криминологический и уголовно-правовой анализ ситуации / А. И. Коробеев, Р. И. Дремлюга, Я. О. Кучина. – Текст : непосредственный // Всероссийский криминологический журнал. – 2019. – № 3. – С. 416–425.

184. *Кузнецов, П. С.* Причины роста преступлений в сфере компьютерной информации в современной России / П. С. Кузнецов. – Текст : непосредственный // Вестник магистратуры. – 2020. – № 4–3. – С. 73–75.

185. *Кузнецова, Е. В.* Информационное пространство сети Интернет в системе детерминант преступности несовершеннолетних / Е. В. Кузнецова. – Текст : непосредственный // Вестник Московского университета МВД России. – 2015. – № 9. – С. 71–74.

186. *Кучерков, И. А.* О понятии «киберпреступление» в законодательстве и научной доктрине / И. В. Кучерков. – Текст : непосредственный // Юридическая наука. – 2019. – № 10. – С. 78–81.

187. *Леонова, А. А.* Актуальные вопросы профилактики правонарушений, совершаемых с использованием дистанционных технологий / А. А. Леонова, М. Е. Архипов, А. С. Оюн, В. А. Шумская. – Текст : непосредственный // Правовая позиция. – 2023. – № 5(41). – С. 57–62.

188. *Майстренко, Г. А.* Киберпреступность в России: сущность, общественная опасность и методы борьбы / Г. А. Майстренко. – Текст : непосредственный // Вопросы российского и международного права. – 2022. – Т. 12, № 1А. – С. 181–186.

189. *Макушев, Д. И.* Криминологическая характеристика личности киберпреступника / Д. И. Макушев. – Текст : непосредственный // Актуальные проблемы гуманитарных и естественных наук. – 2016. – № 1–3. – С. 202–204.

190. *Мерзлов, Ю. А.* Криминологический портрет лиц, совершающих преступления в сфере компьютерной информации / Ю. А. Мерзлов. – Текст : непосредственный // Правопорядок: история, теория, практика. – 2015. – № 4(7). – С. 56–61.
191. *Молоков, В. В.* Киберпреступность: анализ и региональные особенности / В. В. Молоков. – Текст : непосредственный // Вестник Сибирского юридического института МВД России. – 2022. – № 4(49). – С. 171–175.
192. *Мороз, Н. О.* Деятельность Интерпола по координации сотрудничества в борьбе с преступностью в сфере высоких технологий / Н. О. Мороз. – Текст : непосредственный // Вестник Полоцкого государственного университета. Серия D: «Экономические и юридические науки». – 2011. – № 14. – С. 147–148.
193. *Мухамеджанова, А. Д.* Особенности динамики киберпреступности в Республике Казахстан и ее влияние на вопросы ее предупреждения / А. Д. Мухамеджанова. – Текст : непосредственный // Российско-азиатский правовой журнал. – 2022. – № 2. – С. 49–55.
194. *Номоконов, В. А.* Актуальные проблемы борьбы с киберпреступностью / В. А. Номоконов. – Текст : непосредственный // Информационные технологии и безопасность : сб. науч. тр. междунар. конф. – Киев : Национальная академия наук Украины, 2003. – Вып. 3. – С. 105.
195. *Номоконов, В. А.* Киберпреступность как новая криминальная угроза / В. А. Номоконов, Т. Л. Тропина. – Текст : непосредственный // Криминология: вчера, сегодня, завтра. – 2012. – № 1. – С. 42–55.
196. *Омигов, В. И.* Некоторые формы и содержание прогноза развития преступности в России / В. И. Омигов. – Текст : непосредственный // Российский следователь. – 2016. – № 14. – С. 35–38.
197. *Оссама, К. Е. А.* Предупреждение киберпреступлений в США и России: криминологическая характеристика личности киберпреступника в США / К. Е. А. Оссама. – Текст : непосредственный // Евразийский юридический журнал. – 2022. – № 2(165). – С. 324–325.

198. *Пархоменко, С. В.* Предупреждение компьютерной преступности в Российской Федерации: интегративный и комплексные подходы / С. В. Пархоменко, К. Н. Евдокимов. – Текст : непосредственный // Всероссийский криминологический журнал. – 2015. – Т. 9, № 2. – С. 265–276.

199. *Петровский, А. В.* Преступное поведение как криминологическая категория и объект антикриминального предупредительного воздействия / А. В. Петровский. – Текст : непосредственный // Журнал правовых и экономических исследований. – 2024. – № 4. – С. 179–185.

200. *Пинкевич, Т. В.* Цифровое неравенство как фактор преступности / Т. В. Пинкевич. – Текст : непосредственный // Виктимология. – 2024. – Т. 11, № 4. – С. 538–545.

201. *Пинкевич, Т. В.* Современные угрозы криминологической безопасности России / Т. В. Пинкевич. – Текст : непосредственный // Философия права. – 2021. – № 3 (98). – С. 91 – 95.

202. *Прозументов, Л. М.* Криминализация и декриминализация как средства выражения уголовно-правовой политики / Л. М. Прокументов. – Текст : непосредственный // Вопросы развития российского законодательства : сб. мат-лов регион. науч.-практ. конф. – Томск : Издательство научно-технической литературы, 2005. – С. 132–133.

203. *Прозументов, Л. М.* Некоторые подходы к рассмотрению детерминант преступности в отечественной криминологии / Л. М. Прокументов, А. В. Шеслер. – Текст : непосредственный // Вестник Томского государственного университета. – 2017. – № 420. – С. 160–166.

204. *Пучков, Д. В.* Киберпреступность как негативное специфическое явление современного общества / Д. В. Пучков – Текст : непосредственный // Евразийский юридический журнал. – 2017. – № 12. – С. 207–210.

205. *Пучков, Д. В.* Основные тенденции развития международной преступности в сфере реализации кибертехнологий / Д. В. Пучков. – Текст : непосредственный // Общество и право. – 2019. – № 2(68). – С. 41–45.

206. *Пучков, Д. В.* Состояние уголовно-правового регулирования киберпреступлений в уголовном законодательстве Российской Федерации / Д. В. Пучков. – Текст : непосредственный // Правовая политика и правовая жизнь. – 2019. – № 1. – С. 63–71.

207. *Репецкая, А. Л.* Современное состояние, структура и тенденции российской преступности / А. Л. Репецкая. – Текст : непосредственный // Вестник Омского университета. Серия «Право». – 2018. – № 1(54). – С. 151–156.

208. *Романенко, А. С.* Некоторые аспекты борьбы с киберпреступностью / А. С. Романенко. – Текст : непосредственный // Уголовный закон Российской Федерации: проблемы правоприменения и перспективы совершенствования : материалы всерос. круглого стола. – Иркутск : Восточно-Сибирский институт МВД России, 2015. – Вып. 6. – С. 196–199.

209. *Рустимова, Г. Р.* Профилактика уголовных правонарушений в сфере информатизации и связи в Республике Казахстан / Г. Р. Рустимова. – Текст : непосредственный // Вестник Могилевского института МВД. – 2020. – № 1. – С. 58–63.

210. *Сабиров, К. К.* Некоторые вопросы законодательного укрепления кибербезопасности в Республике Казахстан / К. К. Сабиров, Ф. Р. Ахмеджанов. – Текст : непосредственный // Вопросы кибербезопасности. – 2017. – № 3(21). – С. 55–62.

211. *Сафин, Ф. Ю.* О некоторых особенностях личностной характеристики современного киберпреступника / Ф. Ю. Сафин. – Текст : непосредственный // Закон. Право. Государство. – 2022. – № 4(36). – С. 136–139.

212. *Север, Н. С.* Некоторые особенности личности «киберпреступников»: криминологический аспект / Н. С. Север. – Текст : непосредственный // Молодой ученый. – 2022. – № 53. – С. 87–91.

213. *Север, Н. С.* Особенности криминологической характеристики личности киберпреступников / Н. С. Север. – Текст : непосредственный // Вестник Волгоградского государственного университета. Серия 9, Исследования молодых ученых. – 2022. – № 20. – С. 108–110.

214. *Сидорова, Е. З.* О современных мерах предупреждения преступности / Е. З. Сидорова. – Текст : непосредственный // Современная наука. – 2024. – № 4. – С. 17–50.

215. *Сидорова, Е. З.* Современный понятийный аппарат киберпреступности / Е. З. Сидорова. – Текст : непосредственный // Вестник Тюменского института повышения квалификации сотрудников МВД России. – 2024. – № 1(22). – С. 64–68.

216. *Симонян, К. Р.* Правовое воздействие на личность: сущность и механизм реализации / К. Р. Симонян. – Текст : непосредственный // Юридический вестник Кубанского государственного университета. – 2023. – № 4. – С. 21–28.

217. *Старостенко, О. А.* Профилактика и предупреждение кибермошенничества / О. А. Старостенко. – Текст : непосредственный // Наука. Образование. Современность. – 2020. – № 1–2. – С. 41–44.

218. *Степанов-Егиянц, В. Г.* К вопросу о месте совершения компьютерных преступлений / В. Г. Степанов-Егиянц. – Текст : непосредственный // Армия и общество. – 2014. – № 5. – С. 16–19.

219. *Суходолова, Ю. К.* Уголовно-правовой аспект учета личности преступников, использующих информационные технологии / Ю. К. Суходолова. – Текст : непосредственный // Вестник Волгоградского государственного университета. Серия 9 : Исследования молодых ученых. – 2022. – № 20. – С. 111–113.

220. *Сыздыков, А. Ж.* Криминологический портрет киберпреступника / А. Ж. Сыздыков, Н. К. Имангалиев. – Текст : непосредственный // Наука и жизнь Казахстана. – 2018. – № 5(65). – С. 55–59.

221. *Талан, М. В.* Криминологический анализ личности мошенника в сфере неправомерного использования электронных средств платежа / М. В. Талан, Б. Э. Шавалеев. – Текст : непосредственный // Вестник Санкт-Петербургского университета. Право. – 2023. – № 1. – С. 108–122.

222. Толыбаева, А. А. Цифровая грамотность сотрудников правоохранительных органов при противодействии онлайн-мошенничеству / А. А. Толыбаева, Г. Р. Рустемова. – Текст : непосредственный // Информатизация и информационная безопасность правоохранительных органов : сб. тр. Междунар. науч.-практ. конф. – Москва: Академия управления МВД России, 2024. – С. 298–311.

223. Тропина, Т. Л. Киберпреступность и кибертерроризм / Т. Л. Тропина. – Текст : непосредственный // Организованная преступность, терроризм и коррупция. Криминологический ежеквартальный альманах. – 2003. – № 2. – С. 140–144.

224. Чекунов, И. Г. Киберпреступность: понятие, классификация, современные вызовы и угрозы / И. Г. Чекунов. – Текст : непосредственный // Молодые ученые. – 2012. – № 3. – С. 178–186.

225. Чекунов, И. Г. Киберпреступность: проблемы и пути их решения / И. Г. Чекунов. – Текст : непосредственный // Вестник Академии права и управления. – 2017. – № 25. – С. 97–103.

226. Чернякова, А. В. Международный и зарубежный опыт уголовно-правового противодействия хищениям, совершаемых с использованием компьютерной информации / А. В. Чернякова. – Текст : непосредственный // Юридическая наука и правоохранительная практика. – 2018. – № 4. – С. 168–175.

227. Шарыпова, Т. Н. Киберпреступность в XXI веке / Т. Н. Шарыпова, А. А. Сидоренко. – Текст : непосредственный // Аллея науки. – 2019. – Т. 2, № 1(28). – С. 978–981.

228. Якимова, Е. М. Международное сотрудничество в борьбе с киберпреступностью / Е. М. Якимова, С. В. Нарутто. – Текст : непосредственный // Всероссийский криминологический журнал. – 2016. – № 2. – С. 369–378.

229. *Kshetri, N.* Cybercrime and cybersecurity in india: causes, consequences and implications for the future / N. Kshetri // *Crime, Law and Social Change*. – 2016. – № 66. – P. 315–320.

230. *Pratt, T. C.* Routine online activity and internet fraud targeting: extending the generality of routine activity theory / T. C. Pratt, K. Holtfreter, M. D. Reisig // *Journal of Research in Crime and Delinquency*. – 2010. – № 47. – P. 270–281.

Диссертации и авторефераты диссертаций

231. *Аратулы, К.* Уголовная политика в борьбе с компьютерной преступностью в условиях глобализации (на казахском языке) : дис. ... д-ра философии (PhD) / Аратулы Куаныш. – Алматы, 2013. – 166 с. – Текст : непосредственный.

232. *Бражник, С. Д.* Преступления в сфере компьютерной информации: проблемы законодательной техники : дис. ... канд. юрид. наук : 12.00.08 / Бражник Сергей Дмитриевич. – Ижевск, 2002. – 189 с. – Текст : непосредственный.

233. *Бытко, С. Ю.* Некоторые проблемы уголовной ответственности за преступления, совершаемые с использованием компьютерных технологий : дис. ... канд. юрид. наук : 12.00.08 / Бытко Сергей Юрьевич. – Саратов, 2002. – 204 с. – Текст : непосредственный.

234. *Воробьев, В. В.* Преступления в сфере компьютерной информации (юридическая характеристика и квалификация) : дис. ... канд. юрид. наук : 12.00.08 / Воробьев Виктор Викторович. – Нижний Новгород, 2000. – 201 с. – Текст : непосредственный.

235. *Гаджиев, М. С.* Криминологический анализ преступности в сфере компьютерной информации (по материалам Республики Дагестан) : дис. ... канд. юрид. наук : 12.00.08 / Гаджиев Марат Салахетдинович. – Махачкала, 2004. – 168 с. – Текст : непосредственный.

236. *Геллер, А. В.* Уголовно-правовые и криминологические аспекты обеспечения защиты электронной информации и Интернета : дис. ... канд. юрид.

наук : 12.00.08 / Геллер Артем Владимирович. – Москва, 2006. – 216 с. – Текст : непосредственный.

237. *Добровольский, Д. В.* Актуальные проблемы борьбы с компьютерной преступностью : дис. ... канд. юрид. наук : 12.00.08 / Добровольский Дмитрий Владимирович. – Москва, 2005. – 218 с. – Текст : непосредственный.

238. *Доронин, А. М.* Уголовная ответственность за неправомерный доступ к компьютерной информации : дис. ... канд. юрид. наук : 12.00.08 / Доронин Андрей Михайлович. – Москва, 2003. – 154 с. – Текст : непосредственный.

239. *Евдокимов, К. Н.* Противодействие компьютерной преступности: теория, законодательство, практика: дис. ... д-ра юрид. наук : 12.00.08 / Евдокимов Константин Николаевич. – Москва, 2021. – 557 с. – Текст : непосредственный.

240. *Жмыхов, А. А.* Компьютерная преступность за рубежом и ее предупреждение : дис. ... канд. юрид. наук : 12.00.08 / Жмыхов Александр Александрович. – Москва, 2003. – 178 с. – Текст : непосредственный.

241. *Зыков, Д. А.* Виктимологические аспекты предупреждения компьютерного мошенничества : дис. ... канд. юрид. наук : 12.00.08 / Зыков Даниил Алексеевич. – Владимир, 2002. – 211 с. – Текст : непосредственный.

242. *Кесарева, Т. П.* Криминологическая характеристика и предупреждение преступности в российском сегменте сети Интернет : дис. ... канд. юрид. наук : 12.00.08 / Кесарева Татьяна Петровна. – Москва, 2002. – 195 с. – Текст : непосредственный.

243. *Конев, Д. А.* Криминологическая безопасность и ее обеспечение в сфере цифровых технологий: дис. ... канд. юрид. наук : 12.00.08 / Конев Денис Андреевич. – Омск, 2022. – 206 с. – Текст : непосредственный.

244. *Красненкова, Е. В.* Обеспечение информационной безопасности в Российской Федерации уголовно-правовыми средствами : дис. ... канд. юрид. наук : 12.00.08 / Красненкова Елена Валерьевна. – Москва, 2006. – 188 с. – Текст : непосредственный.

245. *Лопатина, Т. М.* Криминологические и уголовно-правовые основы противодействия компьютерной преступности : дис. ... д-ра юрид. наук : 12.00.08 / Лопатина Татьяна Михайловна. – Москва, 2006. – 418 с. – Текст : непосредственный.

246. *Нурпеисова, А. К.* Уголовно-правовые и криминалистические аспекты компьютерной преступности : автореф. дис. ... канд. юрид. наук : 12.00.08 / Нурпеисова Алма Кабикешевна. – Караганда, 2010. – 33 с. – Текст : непосредственный.

247. *Простосердов, М. А.* Экономические преступления, совершаемые в киберпространстве, и меры противодействия им : дис. ... канд. юрид. наук : 12.00.08 / Простосердов Михаил Александрович. – Москва, 2016. – 232 с. – Текст : непосредственный.

248. *Родина, Е. А.* Противодействие криминальной виктимизации пользователей сети „Интернет“ в киберпространстве : дис. ... канд. юрид. наук : 5.1.4 / Родина Екатерина Анатольевна. – Саратов, 2022. – 217 с. – Текст : непосредственный.

249. *Сеитов, Т. Б.* Международно-правовое сотрудничество государств в борьбе с компьютерной преступностью : дис. ... канд. юрид. наук : 12.00.10 / Сеитов Талгат Булатович. – Алматы, 2002. – 120 с. – Текст : непосредственный.

250. *Смирнова, Т. Г.* Уголовно-правовая борьба с преступлениями в сфере компьютерной информации : дис. ... канд. юрид. наук : 12.00.08 / Смирнова Татьяна Георгиевна. – Москва, 1998. – 161 с. – Текст : непосредственный.

251. *Старичков, М. В.* Умышленные преступления в сфере компьютерной информации: уголовно-правовая и криминологическая характеристики : дис. ... канд. юрид. наук : 12.00.08 / Старичков Максим Владимирович. – Иркутск, 2006. – 237 с. – Текст : непосредственный.

252. *Степанов-Егиянц, В. Г.* Преступления в сфере безопасности обращения компьютерной информации: сравнительный анализ : дис. ... канд. юрид. наук : 12.00.08 / Степанов-Егиянц Владимир Георгиевич. – Москва, 2005. – 168 с. – Текст : непосредственный.

253. *Толеубекова, Б. Х.* Проблемы совершенствования борьбы с преступлениями, совершаемыми с использованием компьютерной техники : дис. ... д-ра юрид. наук : 22.00.04 / Толеубекова Бахиджан Хасеновна. – Алматы, 1998. – 380 с. – Текст : непосредственный.

254. *Тропина, Т. Л.* Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы : дис. ... канд. юрид. наук : 12.00.08 / Тропина Татьяна Львовна. – Владивосток, 2005. – 234 с. – Текст : непосредственный.

255. *Тропина, Т. Л.* Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы : автореф. дис. ... канд. юрид. наук : 12.00.08 / Тропина Татьяна Львовна. – Владивосток, 2005. – 26 с. – Текст : непосредственный.

256. *Ушаков, С. И.* Преступления в сфере обращения компьютерной информации (теория, законодательство, практика) : дис. ... канд. юрид. наук : 12.00.08 / Ушаков Сергей Иванович. – Ростов-на-Дону, 2000. – 176 с. – Текст : непосредственный.

257. *Чекунов, И. Г.* Криминологическое и уголовно-правовое обеспечение предупреждения киберпреступности : дис. ... канд. юрид. наук : 12.00.08 / Чекунов Игорь Геннадьевич. – Москва, 2013. – 223 с. – Текст : непосредственный.

258. *Числин, В. П.* Уголовно-правовые меры защиты информации от неправомерного доступа : дис. ... канд. юрид. наук : 12.00.08 / Числин Виталий Петрович. – Москва, 2004. – 134 с. – Текст : непосредственный.

259. *Шарков, А. Е.* Неправомерный доступ к компьютерной информации: преступность деяния и проблемы квалификации : дис. ... канд. юрид. наук : 12.00.08 / Шарков Александр Евгеньевич. – Ставрополь, 2004. – 174 с. – Текст : непосредственный.

260. *Ястребов, Д. А.* Неправомерный доступ к компьютерной информации: уголовно-правовые и криминологические аспекты : дис. ... канд. юрид. наук : 12.00.08 / Ястребов Дмитрий Андреевич. – Москва, 2005. – 243 с. – Текст : непосредственный.

Электронные источники информации

261. *Аратулы, К.* Преступления в сфере компьютерной информации в РК и зарубежных странах / К. Аратулы. – URL: <https://articlekz.com/article/10037>. – Текст : электронный.

262. *В Казахстане* активно растет количество пользователей интернета. – URL: <https://ranking.kz/digest/industries-digest/>. – Текст : электронный.

263. *Выписка* из Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, утвержденной Президентом РФ 12 декабря 2014 г. № К 1274. – URL: <http://www.fsb.ru/> – Текст : электронный.

264. *Киберпреступность*. Модуль 3. Правовая база и права человека // ООН, Вена, 2019. – С. 4. – URL: https://www.unodc.org/documents/e4j/Cybercrime/Cybercrime_Module_3_Legal_Frameworks_and_Human_Rights_RU.pdf. – Текст : электронный.

265. *Козлов, В. Е.* «Computer Crime»: что стоит за названием? / В. Е. Козлов // Центр исследования компьютерной преступности. – URL: <http://www.crime-research.ru/library/CCrime.html>. – Текст : электронный.

266. *Количество* кибератак увеличилось в Казахстане. – URL: https://tengrinews.kz/kazakhstan_news/kolichestvo-kiberatak-uvelichilos-v-kazahstane-430369/. – Текст : электронный.

267. *Машаев, А.* Что стало причиной роста киберкриминала в Казахстане / А. Машаев // Официальный сайт газеты «Курсив». – URL: <https://kz.kursiv.media/2022-12-15/chto-stalo-prichinoj-rosta-kiberkriminala-v-kazahstane/>. – Текст : электронный.

268. *Мошенники* используют нейросети для копирования голоса и образа жертвы. – URL: <https://news.rambler.ru/tech/>. – Текст : электронный.

269. *Отчет DataReportal*: цифровизация России в 2023 году. – URL: <https://drozd.red/blog/marketing/otchet/>. – Текст : электронный.

270. *Решение* No PC.DEC/1202 «Меры укрепления доверия в рамках ОБСЕ с целью сокращения рисков возникновения конфликтов в результате

использования информационных и коммуникационных технологий». ОБСЕ, Постоянный совет. От 10 марта 2016 г. // Официальный сайт ОБСЕ. – URL: «<https://www.osce.org/ru/pc/228521?download=true>». – Текст : электронный.

271. *Россию захлестнула волна IT-преступлений.* – URL: <https://smart-lab.ru/blog/>. – Текст : электронный.

272. *Состояние преступности в России за январь–декабрь 2022 г.* – URL: <http://crimestat.ru/>. – Текст : электронный.

273. *Статистические данные* Главного информационно-аналитического центра Министерства внутренних дел РФ. – URL: https://xn--b1aew.xn--p1ai/mvd/structure1/Centri/Glavnij_informacionno_analiticheskij_cen. – Текст : электронный.

274. *Статистические данные* Министерства внутренних дел Республики Казахстан (МВД РК) – URL: <https://www.gov.kz/memleket/entities/qriim/>. – Текст : электронный.

275. *Статистические данные* Федеральной службы государственной статистики. – URL: <https://rosstat.gov.ru/folder/>. – Текст : электронный.

276. *Статистические данные* – сведения об уголовных правонарушениях за 2022 год. – URL: <https://qamqor.gov.kz>. – Текст : электронный.

277. *TACC: в 2022 году сумма ущерба от IT-преступлений в России выросла на 20%.* – URL: <https://www.gazeta.ru/tech/news/2022/10/19//>. – Текст : электронный.

278. *Токанов, Е. Е.* Криминологический портрет киберпреступника и методы предотвращения преступлений в сфере информатизации и связи / Е. Е. Токанов. – URL: <https://dspace.enu.kz/jspui/bitstream/>. – Текст : электронный.

279. *Топ-5 мошеннических схем с использованием искусственного интеллекта в 2023 году!* – URL: <https://vc.ru/u/1902918-komalenkov-kirill-lirik/>. – Текст : электронный.

280. *Эксперт оценил ущерб от киберпреступлений в России в 2021 году* – Текст : электронный // Официальный канал сайта «Риа новости». – URL: <https://ria.ru/20211222/kiberprestupleniya-1764832102.html/>. – Текст электронный.

ПРИЛОЖЕНИЯ

Приложение 1

Результаты анкетирования населения Российской Федерации о киберпреступности и ее причинах

Таблица 1 – Характеристика личности респондентов, п – 434

Вопрос	Варианты ответа	Результаты (кол-во ответов (%))
1. Ваш пол	Женский	173 (39,86)
	Мужской	261 (60,13)
2. Ваш возраст	20–30 лет	175 (40,32)
	30–40 лет	130 (29,95)
	40–50 лет	86 (19,81)
	50–60 лет	43 (9,9)
	60–70 лет	–
	70–80 лет	–
3. Ваше образование	Неоконченное среднее	–
	Среднее общее	–
	Среднее специальное	44 (10,13)
	Высшее	390 (89,86)
4. Ваш род деятельности	Государственный служащий	347 (79,95)
	Наемный рабочий	34 (7,83)
	Предприниматель	27 (6,22)
	Временно безработный	21 (61,76)
	Другое	5 (1,15)
5. В каком регионе (городе) Вы проживаете?	Алтайский край (Барнаул), Красноярский край, Омская область (Омск), Санкт-Петербург, Москва	

Таблица 2 – Результаты анкетирования

Вопрос	Варианты ответа	Результаты (кол-во ответов (%))
1	2	3
1. Что Вы понимаете под киберпреступностью?	Это интернет-мошенничество	0
	Это все преступления, совершаемые с помощью информационных технологий	390 (89,86)
	Это преступления в сфере информатизации и связи	44 (10,13)
	Ваше мнение	0
2. Как Вы считаете, есть ли опасность в интернете для Вас?	Да	347 (79,95)
	Нет	87 (20,04)
3. Сталкивались ли Вы с киберпреступностью?	Да	342 (78,80)
	Нет	92 (21,19)
4. Как Вы думаете, что толкает человека на совершение киберпреступления?	Несовершенство законодательства	173 (39,86)
	Анонимность сети Интернет	212 (48,84)
	Невостребованность обществом специальных знаний в сфере компьютерных технологий	128 (29,49)
	Ненависть и агрессия	52 (11,98)
	Низкий уровень дохода	260 (59,90)
	Безработица	86 (19,81)
	Низкий уровень культуры	132 (30,41)
	Ваше мнение	0
5. Какой пароль является самым сложным?	Natalia_1993	0
	Iv_08k@*))	434 (100)
	veronica93	0
6. Ваш друг в социальной сети прислал Вам файл и сообщение: «Привет! В этом файле наши с тобой фотки со дня рождения. Смотри!». Но Вы не были с ним на дне рождения. Как Вы поступите?	Открою файл и посмотрю фотографии	12 (2,76)
	Прежде чем открыть файл, зайду в социальную сеть и спрошу у друга, что это за фотографии	75 (17,28)
	Попробую выяснить у друга, не взломан ли его аккаунт	347 (79,95)

1	2	3
7. При загрузке компьютера появляется сообщение: «Ваша операционная система заблокирована. Отправьте смс на номер XXXX и получите код для снятия блокировки». Как Вы поступите?	Перезагружу компьютер – возможно, само пройдет	142 (32,71)
	Скачаю на флешку специальную антивирусную программу, а затем проверю и вылечу с ее помощью компьютер	272 (62,67)
	Отправлю смс на указанный номер, получу код и сниму блокировку	20 (4,60)
8. С помощью чего пользователь может попасть в Интернет?	Гиперссылки	86 (19,81)
	Веб-страницы	45 (10,36)
	Браузера	303 (61,81)
9. Ниже приведены разные категории персональных данных. Какие из них позволяют однозначно идентифицировать человека в Российской Федерации?	Имя, фамилия, год рождения	165 (38,01)
	Фамилия, год рождения, номер школы	0
	Имя, номер паспорта, город проживания	183 (42,16)
	Имя, фамилия, город проживания	0
	Ни один из предложенных вариантов	86 (19,81)
10. Стоит ли пользоваться антивирусной программой?	Да	434 (100)
	Нет	0
11. Какими источниками Вы пользуетесь для получения информации об актуальных новостях?	Телевидение	32 (7,37)
	Печатные издания	0
	Веб-сайты и мобильные приложения официальных СМИ	173 (39,86)
	Новостные сообщества в социальных сетях и мессенджерах (в том числе неофициальных СМИ)	229 (52,76)
12. Знаете ли Вы официальные интернет-ресурсы, куда можно отправить информацию о факте мошенничества в сети Интернет?	Да	181 (41,70)
	Нет	253 (58,29)
13. Оцените, как часто Вы встречаетесь с фейковой (недоверной) информацией в мессенджерах, социальных сетях, на веб-сайтах?	Очень часто (ежедневно)	87 (20,04)
	Часто (еженедельно)	122 (28,11)
	Достаточно часто (ежемесячно)	124 (28,57)
	Редко (за все время встретил 1 раз)	86 (19,81)
	Ни разу не встречал	15 (3,45)

1	2	3
14. Оцените, как часто Вы перепроверяете информацию, опубликованную в мессенджерах, социальных сетях, на веб-сайтах и в иных источниках?	Всегда перепроверяю любую новость	161 (37,09)
	Перепроверяю только информацию из неофициальных источников	193 (44,47)
	Отношусь к этому безразлично	80 (18,43)
15. Оцените, как часто люди из Вашего близкого окружения перепроверяют информацию, опубликованную в мессенджерах, социальных сетях, на веб-сайтах и в иных источниках?	Всегда перепроверяют любую новость	94 (21,65)
	Перепроверяют только информацию из неофициальных источников	161 (37,09)
	Относятся к этому безразлично	179 (41,24)
16. Кому можно передавать данные секретного кода на обороте карты (CVV/CVC)?	Сотрудникам банка	0
	Сотрудникам правоохранительных органов	0
	Друзьям и родственникам	0
	Никому	434 (100)
17. Какие действия необходимо выполнить в случае обнаружения несанкционированных операций по Вашей карте?	Обратиться в банк, который выпустил карту, а затем – в полицию	434 (100)
	Обратиться к родственникам и друзьям	0
	Обратиться к оператору связи	0
	Обратиться в ближайший МФЦ/ЦОН	0
18. На номер Вашего мобильного телефона позвонил человек, который представился сотрудником службы безопасности банка, услугами которого Вы пользуетесь. Он обратился к Вам по имени и сообщил, что банк обнаружил подозрительную операцию, которую пытаются совершить по Вашей карте. Чтобы остановить мошенников, нужно срочно назвать одноразовый пароль, который придет через несколько секунд по смс на номер Вашего телефона. Что бы это значило?	Сотрудник хочет помочь мне, даже позвонил лично, я сейчас же продиктую ему код	0
	Это мошенник! Банки никогда бы не стали торопить своих клиентов и просить назвать им код из смс	307 (70,73)
	Я закончу разговор и позвоню по номеру банка, указанному на обратной стороне карты или официальном сайте	127 (29,26)
	Попрошу его выслать подробности на электронную почту, чтобы продолжить общение там	0
	Продолжу разговор и попытаюсь выяснить подробности происшедшего	0

Результаты анкетирования населения Республики Казахстан о киберпреступности и ее причинах

Таблица 1 – Характеристика личности респондентов, n – 320

Вопрос	Варианты ответа	Результаты (кол-во ответов (%))
1. Ваш пол	Женский	143 (44,69)
	Мужской	177 (55,31)
2. Ваш возраст	20–30 лет	133 (41,56)
	30–40 лет	119 (37,19)
	40–50 лет	46 (14,38)
	50–60 лет	22 (6,88)
	60–70 лет	–
	70–80 лет	–
3. Ваше образование	Неоконченное среднее	–
	Среднее общее	–
	Среднее специальное	32 (10)
	Высшее	288 (90)
4. Ваш род деятельности	Государственный служащий	187 (58,44)
	Наемный рабочий	49 (15,31)
	Предприниматель	47 (14,69)
	Временно безработный	31 (9,69)
	Другое	6 (1,88)
5. В каком регионе (городе) Вы проживаете?	Астана, Актобе, Карагандинская область (Караганда), Талдыкорган, область Жетису	

Таблица 2 – Результаты анкетирования:

Вопрос	Варианты ответа	Результаты (кол-во ответов (%))
1	2	3
1. Что Вы понимаете под киберпреступностью?	Это интернет-мошенничество	9 (2,81)
	Это все преступления, совершаемые с помощью информационных технологий	290 (90,63)
	Это преступления в сфере информатизации и связи	21(6,56)
	Ваше мнение	0

Продолжение таблицы 2

1	2	3
2. Как Вы считаете, есть ли опасность в интернете для Вас?	Да	247 (77,19)
	Нет	73 (22,81)
3. Сталкивались ли Вы с киберпреступностью?	Да	242 (75,62)
	Нет	78 (24,38)
4. Как Вы думаете, что толкает человека на совершение киберпреступления?	Несовершенство законодательства	123 (38,44)
	Анонимность сети Интернет	112 (35,00)
	Невостребованность обществом специальных знаний в сфере компьютерных технологий	98 (30,63)
	Ненависть и агрессия	32 (10,00)
	Низкий уровень дохода	160 (50,00)
	Безработица	66 (20,63)
	Низкий уровень культуры	92 (28,75)
	Ваше мнение	0
5. Какой пароль является самым сложным?	Natalia_1993	0
	Iv_08k@*))	320 (100)
	veronica93	0
6. Ваш друг в социальной сети прислал Вам файл и сообщение: «Привет! В этом файле наши с тобой фотки со дня рождения. Смотри!». Но Вы не были с ним на дне рождения. Как Вы поступите?	Открою файл и посмотрю фотографии	9 (2,21)
	Прежде чем открыть файл, зайду в социальную сеть и спрошу у друга, что это за фотографии	55 (17,19)
	Попробую выяснить у друга, не взломан ли его аккаунт	243 (75,94)
7. При загрузке компьютера появляется сообщение: «Ваша операционная система заблокирована. Отправьте смс на номер XXXX и получите код для снятия блокировки». Как Вы поступите?	Перезагружу компьютер – возможно, само пройдет	124 (38,75)
	Скачаю на флешку специальную антивирусную программу, а затем проверю и вылечу с ее помощью компьютер	161 (50,31)
	Отправлю смс на указанный номер, получу код и сниму блокировку	13 (4,06)
8. С помощью чего пользователь может попасть в Интернет?	Гиперссылки	68 (21,25)
	Веб-страницы	34 (10,63)
	Браузера	201 (62,81)

1	2	3
9. Ниже приведены разные категории персональных данных. Какие из них позволяют однозначно идентифицировать человека в Республике Казахстан?	Имя, фамилия, год рождения	97 (33,31)
	Фамилия, год рождения, номер школы	0
	Имя, номер паспорта, город проживания	156 (48,75)
	Имя, фамилия, город проживания	0
	Ни один из предложенных вариантов	67 (20,94)
10. Стоит ли пользоваться антивирусной программой?	Да	320 (100)
	Нет	0
11. Какими источниками Вы пользуетесь для получения информации об актуальных новостях?	Телевидение	23 (7,19)
	Печатные издания	0
	Веб-сайты и мобильные приложения официальных СМИ	135 (42,19)
	Новостные сообщества в социальных сетях и мессенджерах (в том числе неофициальных СМИ)	162 (50,63)
12. Знаете ли Вы официальные интернет-ресурсы, куда можно отправить информацию о факте мошенничества в сети Интернет?	Да	181 (56,56)
	Нет	139 (43,44)
13. Оцените, как часто Вы встречаетесь с фейковой (недостоверной) информацией в мессенджерах, социальных сетях, на веб-сайтах?	Очень часто (ежедневно)	56 (17,5)
	Часто (еженедельно)	112 (35)
	Достаточно часто (ежемесячно)	97 (30,31)
	Редко (за все время встретил 1 раз)	73 (22,81)
	Ни разу не встречал	12 (3,75)
14. Оцените, как часто Вы перепроверяете информацию, опубликованную в мессенджерах, социальных сетях, на веб-сайтах и в иных источниках?	Всегда перепроверяю любую новость	118 (36,88)
	Перепроверяю только информацию из неофициальных источников	167 (52,19)
	Отношусь к этому безразлично	38 (11,88)
15. Оцените, как часто люди из Вашего близкого окружения перепроверяют информацию, опубликованную в мессенджерах, социальных сетях, на веб-сайтах и в иных источниках?	Всегда перепроверяют любую новость	73 (22,81)
	Перепроверяют только информацию из неофициальных источников	138 (43,12)
	Относятся к этому безразлично	157 (49,06)

1	2	3
16. Кому можно передавать данные секретного кода на обороте карты (CVV/CVC)?	Сотрудникам банка	0
	Сотрудникам правоохранительных органов	0
	Друзьям и родственникам	0
	Никому	320 (100)
17. Какие действия необходимо выполнить в случае обнаружения несанкционированных операций по Вашей карте?	Обратиться в банк, который выпустил карту, а затем – в полицию	320 (100)
	Обратиться к родственникам и друзьям	0
	Обратиться к оператору связи	0
	Обратиться в ближайший МФЦ/ЦОН	0
18. На номер Вашего мобильного телефона позвонил человек, который представился сотрудником службы безопасности банка, услугами которого Вы пользуетесь. Он обратился к Вам по имени и сообщил, что банк обнаружил подозрительную операцию, которую пытаются совершить по Вашей карте. Чтобы остановить мошенников, нужно срочно назвать одноразовый пароль, который придет через несколько секунд по смс на номер Вашего телефона. Что бы это значило?	Сотрудник хочет помочь мне, даже позвонил лично, я сейчас же продиктую ему код	0
	Это мошенник! Банки никогда бы не стали торопить своих клиентов и просить назвать им код из смс	205 (64,06)
	Я закончу разговор и позвоню по номеру банка, указанному на обратной стороне карты или официальном сайте	115 (35,94)
	Попрошу его выслать подробности на электронную почту, чтобы продолжить общение там	0
	Продолжу разговор и попытаюсь выяснить подробности происшедшего	0

Результаты анкетирования сотрудников правоохранительных органов Российской Федерации

Таблица 1 – Характеристика личности респондентов, n – 268

Вопрос	Варианты ответа	Результаты (кол-во ответов (%))
1	2	3
1. Ваш возраст	20–30 лет	134 (50,00)
	30–40 лет	54 (20,14)
	40–50 лет	54 (20,14)
	50–60 лет	26 (9,7)
	60–70 лет	–
2. Ваш стаж работы в следственных или оперативных подразделениях ОВД	до 3 лет	133 (49,62)
	от 3 до 5 лет	32 (11,94)
	от 5 до 10 лет	24 (8,95)
	свыше 10 лет	26 (9,7)
	свыше 20 лет	53 (19,77)
3. В каком регионе (городе) Вы работаете?	Барнаул (27 чел.), Алтайский край (17 чел.), Красноярский край (14 чел.), Омская область (73 чел.), г. Омск (107 чел.), Санкт-Петербург (13 чел.), Москва (17 чел.)	

Таблица 2 – Результаты анкетирования

Вопрос	Вариант ответа	Результаты (кол-во ответов (%))
1. Как Вы оцениваете состояние киберпреступности в регионе, где Вы работаете?	Сверхвысокое	53 (19,77)
	Высокое	134 (50)
	Среднее	81 (30,22)
	Низкое	–
	Иное (укажите)	–
2. Если судить по тем фактическим данным, которые Вам известны, то как можно оценить тенденции киберпреступности?	Увеличивается в геометрической прогрессии	160 (59,7)
	Увеличивается невысокими темпами	108 (40,29)
	Особых изменений нет	–
	Снижается	–
	Иное (укажите)	–

1	2	3
3. По Вашему мнению, возрастает ли общественная опасность киберпреступлений?	Да, общественная опасность таких деяний возрастает	160 (59,7)
	Нет, использование криптовалюты при совершении преступления не оказывает влияния на общественную опасность содеянного	26 (9,7)
	Такие преступления очень сложно выявлять, раскрывать и расследовать	54 (20,14)
	Затрудняюсь ответить	28 (10,44)
	Иное (укажите)	–
4. Как Вы оцениваете нынешнее состояние киберпреступности в России?	Угрожает безопасности России	80 (29,85)
	Является крайне опасным видом преступности	80 (29,85)
	Оказывает влияние в целом на рост преступности	55 (20,52)
	Играет незначительную роль	53 (19,77)
	Не оказывает сколько-нибудь значимого влияния	–
5. Принимали ли Вы участие в раскрытии, расследовании или предупреждении киберпреступлений?	Да	215 (80,22)
	Нет	53 (19,77)
6. Как Вы оцениваете свой уровень знаний о киберпреступлениях?	Высокий	28 (10,44)
	Средний	160 (59,7)
	Низкий	80 (29,85)
	Затрудняюсь ответить	–
	Иное (укажите)	–
7. Укажите источник(и) Вашей осведомленности о киберпреступлениях?	Данные статистической отчетности МВД России	187 (69,77)
	Данные статистической отчетности МВД, ГУВД, УВД субъекта РФ	80 (29,85)
	Материалы судебной практики	107(39,92)
	Личная профессиональная деятельность	160 (59,7)
	Учебно-научная литература (учебники, комментарии, монографии, статьи)	80 (29,85)
	Нормативные правовые источники	53 (19,77)
	Служебно-методические рекомендации	26 (9,7)
	Мнения и знания коллег	53 (19,77)
	Сообщения средств массовой информации	80 (29,85)
	Иное (укажите)	27 (10,07)

Продолжение таблицы 2

1	2	3
8. Как часто в своей профессиональной деятельности Вы сталкивались с киберпреступлениями?	Очень часто	29 (10,82)
	Часто	134 (50)
	Редко	79 (29,41)
	Очень редко	26 (9,7)
	Никогда не сталкивался	–
9. Какие факторы, на Ваш взгляд, затрудняют деятельность по выявлению, раскрытию и расследованию киберпреступлений?	Конструктивные недостатки уголовно-правовых норм, устанавливающих ответственность за киберпреступления	27 (10,07)
	Чрезмерная сложность и запутанность уголовного законодательства	53 (19,77)
	Отсутствие сложившейся судебной практики	53 (19,77)
	Несовершенство уголовно-процессуального законодательства	53 (19,77)
	Несовершенство законодательства об оперативно-розыскной деятельности	–
	Сложности при производстве различного рода экспертиз, исследований	81 (30,22)
	Сложности установления свидетельской базы	54 (20,14)
	Отсутствие реальной технической возможности определения электронных адресов субъектов преступлений	214 (79,85)
	Иное (укажите)	–
10. Какие меры, на Ваш взгляд, будут способствовать повышению эффективности противодействия киберпреступлениям?	Изменения уголовного законодательства в сторону его упрощения	107 (39,92)
	Усиление репрессивных мер в отношении лиц, совершивших киберпреступления	81 (30,22)
	Изменения уголовно-процессуального законодательства и законодательства об ОРД в области расширения полномочий правоохранительных органов	81 (30,22)
	Осуществление программ просвещения в области защиты личности, общества и государства	107 (39,92)

Продолжение таблицы 2

1	2	3
	Привлечение средств массовой информации к пропаганде и систематическому освещению вопросов цифровой грамотности	134 (50,00)
	Правовая поддержка населения	107(39,92)
	Мобилизация организационных ресурсов органов внутренних дел	107(39,92)
	Проведение периодических оперативно-профилактических мероприятий с привлечением сотрудников других контролирующих органов	53 (19,77)
	Иное (укажите)	27 (10,07)
11. Какие меры профилактики Вы предлагали после расследования киберпреступлений (для следователей)?	Профилактика населения, Получение образования / прохождение курсов повышения квалификации в сфере IT сотрудникам ОВД	
12. Как Вы оцениваете состояние киберпреступности в Республике Казахстан?	Угрожает безопасности соседних государств	53 (19,77)
	Является крайне опасным видом преступности	26 (9,7)
	Оказывает влияние в целом на рост преступности	80 (29,85)
	Играет незначительную роль	27 (10,07)
	Не оказывает сколько-нибудь значимого влияния	27 (10,07)
	Иное (укажите)	53 (19,77)
13. Как оцениваете взаимодействие между правоохранительными органами России и Казахстана?	На работе не сталкивался с этим вопросом	187 (69,77)
	Крайне редко обращаются из соседних государств	26 (9,7)
	Взаимодействие находится на ненадлежащем уровне	27 (10,07)
	Система взаимодействия налажена на высоком уровне	0
	Иное (укажите)	28 (10,44)

Результаты анкетирования сотрудников правоохранительных органов Республики Казахстан

Таблица 1 – Характеристика личности респондентов, n – 243

Вопрос	Варианты ответа	Результаты (кол-во ответов (%))
1. Ваш возраст	20–30 лет	97 (39,91)
	30–40 лет	–
	40–50 лет	121 (49,79)
	50–60 лет	25 (10,28)
	60–70 лет	–
2. Ваш стаж работы в следственных или оперативных подразделениях ОВД	до 3 лет	111 (45,67)
	от 3 до 5 лет	27 (11,11)
	от 5 до 10 лет	73 (30,04)
	свыше 10 лет	32 (13,16)
	свыше 20 лет	–
В каком регионе (городе) Вы работаете?	Астана (47 чел.), Актобе (34 чел.), Караганда (58 чел.), Карагандинская область (38 чел.), Талдыкорган (42 чел.), область Жетису (24 чел.)	

Таблица 2 – Результаты анкетирования

Вопрос	Вариант ответа	Результаты (кол-во ответов (%))
1	2	3
1. Как Вы оцениваете состояние киберпреступности в регионе, где Вы работаете?	Сверхвысокое	27 (11,11)
	Высокое	121 (49,79)
	Среднее	63 (25,92)
	Низкое	32 (13,16)
	Иное (укажите)	–
2. Если судить по тем фактическим данным, которые Вам известны, то как можно оценить тенденции киберпреступности?	Увеличивается в геометрической прогрессии	167 (68,72)
	Увеличивается невысокими темпами	43 (17,69)
	Особых изменений нет	21 (8,64)
	Снижается	12 (4,93)
	Иное (укажите)	–

1	2	3
3. По Вашему мнению, возрастает ли общественная опасность киберпреступлений?	Да, общественная опасность таких деяний возрастает	187 (76,95)
	Нет, использование криптовалюты при совершении преступления не оказывает влияния на общественную опасность содеянного	24 (9,87)
	Такие преступления очень сложно выявлять, раскрывать и расследовать	32 (13,16)
	Затрудняюсь ответить	—
	Иное (укажите)	—
4. Как Вы оцениваете нынешнее состояние киберпреступности в Республике Казахстан?	Угрожает безопасности Республики Казахстан	98 (40,32)
	Является крайне опасным видом преступности	26 (10,69)
	Оказывает влияние в целом на рост преступности	119 (48,97)
	Играет незначительную роль	—
	Не оказывает сколько-нибудь значимого влияния	—
5. Принимали ли Вы участие в раскрытии, расследовании или предупреждении киберпреступлений?	Да	194 (79,83)
	Нет	49 (20,16)
6. Как Вы оцениваете свой уровень знаний о киберпреступлениях?	Высокий	0
	Средний	218 (89,71)
	Низкий	4 (1,64)
	Затрудняюсь ответить	21 (8,64)
	Иное (укажите)	—
7. Укажите источник(и) Вашей осведомленности о киберпреступлениях?	Данные статистической отчетности МВД РК	95 (39,09)
	Данные статистической отчетности МВД РК, ДП областей (городов)	121 (49,79)
	Материалы судебной практики	43 (17,69)
	Личная профессиональная деятельность	52 (21,39)
	Учебно-научная литература (учебники, комментарии, монографии, статьи)	52 (21,39)
	Нормативные правовые источники	52 (21,39)
	Служебно-методические рекомендации	0

Продолжение таблицы 2

1	2	3
	Мнения и знания коллег	23 (9,46)
	Сообщения средств массовой информации	121 (49,79)
	Иное (укажите)	–
8. Как часто в своей профессиональной деятельности Вы сталкивались с киберпреступлениями?	Очень часто	73 (30,04)
	Часто	106 (43,62)
	Редко	31 (12,75)
	Очень редко	21 (8,64)
	Никогда не сталкивался	12 (4,93)
9. Какие факторы, на Ваш взгляд, затрудняют деятельность по выявлению, раскрытию и расследованию киберпреступлений?	Конструктивные недостатки уголовно-правовых норм, устанавливающих ответственность за киберпреступления	93 (38,27)
	Чрезмерная сложность и запутанность уголовного законодательства	52 (21,39)
	Отсутствие сложившейся судебной практики	32 (13,16)
	Несовершенство уголовно-процессуального законодательства	0
	Несовершенство законодательства об оперативно-розыскной деятельности	52 (21,39)
	Сложности при производстве различного рода экспертиз, исследований	37 (15,22)
	Сложности установления свидетельской базы	93 (38,27)
	Отсутствие реальной технической возможности определения электронных адресов субъектов преступлений	174 (71,6)
	Иное (укажите)	–
10. Какие меры, на Ваш взгляд, будут способствовать повышению эффективности противодействия киберпреступлениям?	Изменения уголовного законодательства в сторону его упрощения	0
	Усиление репрессивных мер в отношении лиц, совершивших киберпреступления	53 (21,81)
	Изменения уголовно-процессуального законодательства и законодательства об ОРД в области расширения полномочий правоохранительных органов	32 (13,16)
	Осуществление программ просвещения в области защиты личности, общества и государства	121 (49,79)

1	2	3
	Привлечение средств массовой информации к пропаганде и систематическому освещению вопросов цифровой грамотности	121 (49,79)
	Правовая поддержка населения	61 (25,1)
	Мобилизация организационных ресурсов органов внутренних дел	31 (12,75)
	Проведение периодических оперативно-профилактических мероприятий с привлечением сотрудников других контролирующих органов	93 (38,27)
	Иное (укажите)	–
11. Какие меры профилактики Вы предлагали после расследования киберпреступлений (для следователей)?	Меры профилактики и предупреждения киберпреступности	
12. Как Вы оцениваете состояние киберпреступности в Российской Федерации?	Угрожает безопасности соседних государств	97 (39,91)
	Является крайне опасным видом преступности	27 (11,11)
	Оказывает влияние в целом на рост преступности	119 (48,97)
	Играет незначительную роль	–
	Не оказывает сколько-нибудь значимого влияния	–
	Иное (укажите)	–
13. Как оцениваете взаимодействие между правоохранительными органами России и Казахстана?	На работе не сталкивался с этим вопросом	71 (29,21)
	Крайне редко обращаются из соседних государств	92 (37,86)
	Взаимодействие находится на ненадлежащем уровне	27 (11,11)
	Система взаимодействия налажена на высоком уровне	53 (21,81)
	Иное (укажите)	–

Результаты анализа приговоров судов

В ходе проведения исследования были изучены данные, полученные в результате изучения 316 приговоров районных, городских и областных судов Омской, Курганской, Новосибирской, Иркутской областей РФ и Актыбинской, Костанайской, Карагандинской областей РК по делам о преступлениях, предусмотренных ст. ст. 158, 159, 159³, 159⁶, 171², 205², 228¹, 242, 242¹, 242², 272, 273 УК РФ и п. 4 ч. 2 ст. 188, п. 4 ч. 2 ст. 190, ст. ст. 205, 210, ч. 2 ст. 256, п. 5 ч. 3 ст. 297, п. 3 ч. 2 ст. 299, п. 4 ч. 2 ст. 299-1, п. 4 ч. 3 ст. 301, ст. ст. 311, 312 УК РК.

Норма УК РФ	Норма УК РК	Количество изученных приговоров		Средний материальный ущерб, причиненный совершенным преступлением, руб./тенге		Общий материальный ущерб, причиненный совершенным преступлением, руб./тенге	
		РФ	РК	РФ	РК	РФ	РК
ст. 158	п. 4 ч. 2 ст. 188	18	20	118 218	766 416	21 292 017	120 017 753
ст. 159	п. 4 ч. 2 ст. 190	27	59	1 651 014	12 012 263	112 906 000	852 083 020
ст. 159 ³	—	11	—	22 290	—	2 271 100	—
ст. 159 ⁶	—	15	—	1 203 372	—	82 607 000	—
ст. 171 ²	—	9	—	103 530	—	3 899 100	—
ст. 205 ²	ч. 2 ст. 256	11	—	—	—	—	—

ст. 228 ¹	п. 5 ч. 3 ст. 297; п. 3 ч. 2 ст. 299; п. 4 ч. 2 ст. 299-1; п. 4 ч. 3 ст. 301	17	37	—	—	—	—
ст. 242	ст. 311, ст. 312	14	25	—	—	—	—
ст. 242 ¹	—	11	—	—	—	—	—
ст. 272	ст. 205	9	10	7 001 112	46 697 417	103 171 470	588 153 704
ст. 273	ст. 210	11	12	33 930 117	224 303 880	739 626 960	933 111 923
Всего		153	163				

**Характеристика
субъектов киберпреступлений на основе анализа приговоров судов РФ и РК**

Норма УК РФ/ УК РК	Всего	Пол		Возраст				Образование					Место работы		
		Мужской	Женский	14–18 лет	18–35 лет	35–65 лет	Старше 65 лет	Среднее	Среднее специальное	Высшее	Несколько высших	Без образования	Официально не трудоустроен, но имеет постоянный источник доходов	Официально трудоустроен	Не имеет постоянного источника доходов
ст. 158 УК РФ	18	13	5	2	12	4	-	2	11	5	-	-	9	7	2
ст. 159 УК РФ	27	21	6	5	17	3	-	5	13	7	2	-	13	6	8
ст. 159 ³ УК РФ	11	7	4	3	6	2	-	3	6	2	-	-	5	4	2
ст. 159 ⁶ УК РФ	15	12	3	2	11	2	-	2	8	3	2	-	8	4	3
п. 4 ч. 2 ст. 188 УК РК	20	17	3	4	13	3	-	4	12	4	-	-	11	5	4
п. 4 ч. 2 ст. 190 УК РК	59	49	10	6	45	8	-	5	25	20	9	-	27	18	14