Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Пензенский государственный университет»

Юридический институт Кафедра «Уголовное право»
(наименование)

Направление подготовки 40.03.01 Юриспруденция
(код) (наименование)

Профиль «Правозащитная деятельность»
(наименование)

БАКАЛАВРСКАЯ РАБОТА

по теме: «Мошенничество в цифровом пространстве»

Студентка 22ЮЮ2 _____ Авдеева Диана Викторовна
номер группы подпись, дата фамилия, имя, отчество полностью

Научный руководитель к.ю.н., доцент
должность

кафедры «УП» ФГБОУ ВО ПГУ _____ Живодрова Н.А.
наименование организации подпись, дата фамилия, инициалы

Консультанты:

по _____ _____ _____
наименование раздела, звание, должность подпись, дата фамилия, инициалы

по _____ _____ _____
наименование раздела, звание, должность подпись, дата фамилия, инициалы

по _____ _____ _____
наименование раздела, звание, должность подпись, дата фамилия, инициалы

Нормоконтролер: доцент кафедры «УП» _____ Живодрова Н.А.
должность подпись, дата фамилия, инициалы

Работа допущена к защите в (протокол заседания кафедры от _____ 2026 № _)

Заведующий кафедрой «Уголовное право» _____ Рыжова О.А.
название подпись, дата фамилия, инициалы

Работа защищена с оценкой _____ (Протокол от ___ _____ 2026 г. №___)

Секретарь ГЭК _____ Антипкина Е.Г.
подпись, дата фамилия, инициалы

Пенза, 2026 г.

ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Юридический институт

Направление 40.03.01 «Юриспруденция»

Профиль «Правозащитная деятельность»

УТВЕРЖДАЮ
И.о. зав. кафедрой «Уголовное право»
_____/ О.А. Рыжова /
(подпись) (и.о. фамилия)
_____ 2026 г.

ЗАДАНИЕ
на выпускную квалификационную работу студентки гр. № 22 ЮЮ 2
Авдеевой Дианы Викторовны

1. Тема работы: Мошенничество в цифровом пространстве

2. Научный руководитель: к.ю.н., доцент каф. УП Живодрова Н. А.

3. Дата выдачи задания: 25.12.2025 г.

4. Срок сдачи студентом законченной работы: 18.05.2026 г.

5. Перечень подлежащих разработке вопросов:

5.1. История развития законодательства об ответственности за киберпреступления

5.2. Понятие, признаки, характеристика мошенничества в цифровом пространстве

5.3. Криминологическая характеристика лиц, совершающих киберпреступления и их жертв

5.4. Анализ состояния и динамики кибермошенничества в Пензенской области информации

5.5. Проблемы и основные направления совершенствования противодействия кибермошенничеству

6. Консультанты по работе, с указанием относящихся к ним разделов работы:

Раздел	Консультант	Подпись, дата	
		Задание выдал	Выполненное задание принял
Введение		25.12.2025 г. Живодрова Н.А.	25.02.2026 г. Живодрова Н.А.
Уголовно правовые аспекты противодействия преступлениям в цифровом пространстве		25.02.2026 г. Живодрова Н.А.	15.03.2026 г. Живодрова Н.А.
Криминологическая характеристика и региональные особенности цифрового мошенничества		15.03.2026 г. Живодрова Н.А.	08.04.2026 г. Живодрова Н.А.
Проблемы и основные направления совершенствования противодействия кибермошенничеству		08.04.2026 г. Живодрова Н.А.	30.04.2026 г. Живодрова Н.А.
Заключение		30.04.2026 г. Живодрова Н.А.	18.05.2026 г. Живодрова Н.А.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ..... 5

1 Уголовно правовые аспекты противодействия преступлениям в цифровом пространстве..... 9

1.1 История развития законодательства об ответственности за киберпреступления..... 9

1.2 Понятие, признаки, характеристика мошенничества в цифровом пространстве 15

2 Криминологическая характеристика и региональные особенности цифрового мошенничества 31

2.1 Криминологическая характеристика лиц, совершающих киберпреступления и их жертв 31

2.2 Анализ состояния и динамики кибермошенничества в Пензенской области..... 43

3 Проблемы и основные направления совершенствования противодействия кибермошенничеству..... 56

ЗАКЛЮЧЕНИЕ 65

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 69

ПРИЛОЖЕНИЯ 76

ВВЕДЕНИЕ

Актуальность настоящего исследования обусловлена тем, что в условиях современной цифровой трансформации общества информационно–телекоммуникационные технологии заняли центральное место в экономических, социальных и личных отношениях. Однако наряду с очевидными преимуществами цифровизация создала благоприятную среду для совершения преступлений нового поколения. Как справедливо отмечал бывший Генеральный секретарь ООН Пан Ги Мун, революция в области ИКТ сопровождается новыми угрозами, связанными с киберпреступностью.[1]

Особую тревогу вызывает то, что одним из наиболее распространенных и динамично развивающихся видов преступлений как в России, так и в мире остается мошенничество. В цифровую эпоху оно неизбежно приобретает дистанционный (виртуальный) характер, а способы его совершения постоянно эволюционируют, что делает традиционные механизмы противодействия малоэффективными.

Согласно данным МВД РФ, в 2023–2025 годах мошенничество остаётся одним из самых распространённых преступлений против собственности, а его цифровые формы выделяются в отдельный значимый массив уголовных дел. Несмотря на небольшое снижение числа зарегистрированных фактов в 2025 году, более половины таких преступлений относятся к тяжким и особо тяжким составам, а средний размер ущерба, особенно по цифровым схемам, неуклонно растёт. Это свидетельствует не только о распространенности данного явления, но и о недостаточности существующих мер борьбы.

В этих условиях ключевое значение приобретает не столько реактивная правоохранительная деятельность, сколько активная разработка мер предупреждения и профилактики. Широкие возможности цифровой экономики все чаще используются как инструмент обмана и злоупотребления

[1] Дрёмин А. А. Современное состояние и динамика преступности мошенничества с использованием электронных средств платежа в 2025 // Вестник науки. – 2025. – № 6. – С. 72.

доверием для хищения денежных средств. В связи с этим возникает объективная потребность в выявлении характерных особенностей составов данных преступлений, личности киберпреступника, а также в информировании населения о способах защиты своих средств при использовании IT–продуктов.[1]

Таким образом, тема «Мошенничество в цифровом пространстве» является высоко актуальной для современной юридической науки и правоприменительной практики, поскольку требует разработки и внедрения универсальных, своевременных и эффективных мер предупреждения, адаптированных к реалиям цифрового мира.

Целью исследования является комплексный уголовно–правовой и криминологический анализ мошенничества в цифровом пространстве, а также разработка на этой основе рекомендаций по совершенствованию мер противодействия данному виду преступлений.

Для достижения указанной цели поставлены следующие задачи:

– изучить историю развития законодательства об ответственности за киберпреступления;

– раскрыть понятие, признаки, характеристику мошенничества в цифровом пространстве;

– представить криминологическую характеристику лиц, совершающих киберпреступления, и их жертв;

– провести анализ состояния и динамики кибермошенничества в Пензенской области за период 2023–2026 годов;

– выявить проблемы и основные направления совершенствования противодействия кибермошенничеству.

Объектом исследования выступают общественные отношения, складывающиеся в сфере противодействия мошенничеству, совершаемому с использованием информационно–телекоммуникационных технологий и в

[1] Витвицкая С. С. Киберпреступления: понятие, классификация, международное противодействие // Правовой порядок и правовые ценности. – 2023. –№ 1. – С. 126.

цифровом пространстве.

Предметом исследования являются правовые отношения, возникающие в сфере совершения и противодействия мошенничеству с использованием информационно–телекоммуникационных технологий.

Научная новизна исследования заключается в комплексном анализе мошенничества в цифровом пространстве через призму уголовно–правовых и криминологических аспектов на основе актуальных статистических данных за 2023–2026 годы, включая региональный материал по Пензенской области.

В процессе работы использовались как общенаучные методы (диалектический, системно–структурный, логический, анализ, синтез, индукция, дедукция), так и частно–научные методы: формально–юридический (при анализе норм УК РФ), сравнительно–правовой (при сопоставлении российского и зарубежного законодательства), статистический (при обработке данных о преступности), криминологический (при изучении личности преступника и жертвы), а также метод документального анализа (при изучении судебной практики и ведомственных отчётов).

Теоретическую основу исследования составили труды отечественных учёных в области уголовного права, криминологии и криминалистики.

Использованы работы Ю. М. Батурина, А. М. Жодзинского, В. А. Номоконова, А. П. Кузнецова, И. А. Кучеркова, посвящённые истории развития законодательства и юридической природе киберпреступлений.

Криминологический аспект основан на публикациях Ю. В. Белевитиной, П. А. Муллаяровой, К. А. Айнутдиновой, раскрывающих личность киберпреступника и виктимологические особенности. Вопросы расследования проанализированы по работам В. В. Полякова, С. В. Зуева, В. Б. Вехова, А. Н. Попова, С. В. Петракова, Т. Н. Уторовой, Л. А. Колпаковой, а также Е. А. Хариной и методическим рекомендациям Генпрокуратуры.

Проблемы противодействия исследованы на основе статей Е. Н. Клещиной, Стратегии развития информационного общества и Доктрины информационной безопасности.

Нормативную основу исследования составили Конституция РФ, Уголовный кодекс РФ, Федеральный закон от 01.04.2025 № 41–ФЗ «О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации», постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно–телекоммуникационных сетей, включая сеть «Интернет», и другие нормативно–правовые акты, посвященные данной проблематике.

Эмпирическую базу – статистические данные МВД России, отчёты по Пензенской области за 2024–2026 годы и материалы судебной практики.

Структура работы обусловлена целью и задачами исследования. Бакалаврская работа состоит из введения, трёх глав, состоящих из пяти параграфов, заключения, списка использованных источников и приложений.

1 Уголовно правовые аспекты противодействия преступлениям в цифровом пространстве

1.1 История развития законодательства об ответственности за киберпреступления

История правового регулирования ответственности за киберпреступления – сравнительно новый, но активно развивающийся сегмент права, который складывался по мере совершенствования информационных технологий. Потребность в сохранении и передаче информации существовала всегда – от древних носителей до печатного станка и радио. Однако именно глобальная сеть Интернет, объединившая мир, открыла ранее недоступные возможности для обмена данными.[1]

Вместе с тем активное внедрение компьютеров в повседневную жизнь породило виды преступлений, которых не знало традиционное право. Сегодня они угрожают не только отдельным лицам, но и общественной безопасности в целом.

Первыми с киберпреступлениями столкнулись США. В 1960–х гг. в американских СМИ появился термин «киберпреступность». После инцидентов (дело А. Конфессоре, 1969 г., и кража из «Секьюрити Пасифик Бэнк») стало очевидно: новые технологии требуют новых правовых средств.

Впервые на общенациональном уровне ответственность за киберпреступления закрепили в Швеции (Data Act, 1973 г.), установив наказание за несанкционированный доступ и ввод ложных данных.

В США длительное время применяли общий закон о почтовом и телеграфном мошенничестве. В 1977 г. принят федеральный закон об уголовной ответственности за киберпреступления, в 1984 г. – Computer Fraud and Abuse Act (впоследствии неоднократно корректировался). В настоящее время обсуждается ужесточение санкций (до 20–30 лет лишения свободы за кибершпионаж и взлом критической инфраструктуры). Отдельные штаты (например, Калифорния) вправе принимать собственные уголовные законы в

[1] Номоконов В. А. Киберпреступность как новая криминальная угроза // Криминология интернет-пространства. - 2012. - № 2. - С.45.

этой сфере.

В Великобритании до 1990–х гг. законодательство было неэффективным. В 1990 г. принят Computer Misuse Act, установивший ответственность за несанкционированный доступ к программам или данным, их изменение, уничтожение, копирование. В 2000 г. киберпространство включено в определение терроризма.

В странах романо–германской правовой семьи (Германия, Нидерланды) акцент сделан на охрану цифровых данных. УК ФРГ предусматривает наказание за изменение, повреждение, удаление данных, а также компьютерный саботаж. В Нидерландах наказания мягче (штрафы, лишение свободы до 6 месяцев). В Ирландии (Акт о криминальном ущербе, 1991 г.) виновным признаётся лицо, использующее компьютер для неправомерного доступа к данным вне зависимости от результата.

Таким образом, анализ зарубежного опыта показывает, что, несмотря на различия в подходах (специальные законы в США и Великобритании, кодифицированные нормы в Германии, относительно мягкие санкции в Нидерландах), все развитые страны признают необходимость уголовно–правовой охраны компьютерной информации.

Стоит отметить, что Российская история законодательства в данной области имеет свои особенности. Первый зафиксированный случай киберпреступления произошёл в Вильнюсе в 1979 году: работница почты использовала брешь в системе «Онега» для кражи денег из пособий и пенсий на 78 тысяч рублей. Этот факт внесли в международный реестр компьютерных преступлений, и тогда возник вопрос о введении уголовной ответственности. Собственного опыта на тот момент не имелось, поэтому обращались к зарубежным наработкам.[1]

Российский законодатель пошёл по пути создания новых норм, хотя в некоторых научных работах изначально предлагалось дополнять существующие составы квалифицирующими признаками, данные предложения были реализованы позже.

Проблема заключалась в том, что до внесения изменений в УК требовалось принять акты, регулирующие саму сферу информации.

[1] Китайкина О. О. Российское законодательство об уголовной ответственности за преступления в сфере компьютерной информации: история и современность // Научный формат. – 2020. – №12(15). – С.20.

23 сентября 1992 года было принято два базовых закона: «О правовой охране программ для электронных вычислительных машин и баз данных» (утратил силу в 2006) и «О правовой охране топологий интегральных микросхем» (утратил силу в 2006). Первый ввёл легальные определения «программы для ЭВМ», «базы данных», «воспроизведения». Второй – «топологии интегральной микросхемы», «интегральной микросхемы». Оба определяли объекты и условия охраны.

Постановление Верховного Совета РФ от 23 сентября 1992 года поручало Правительству до 31 декабря 1992 года внести проекты изменений в ГК и УК РСФСР, но работа затянулась.[1]

Появлению норм о киберпреступлениях предшествовали другие важные акты:

– закон «Об авторском праве и смежных правах» от 9 июля 1993 года (утратил силу в 2004);

– закон РФ от 21 июля 1993 года №5485–I «О государственной тайне» (действует до сих пор).

Федеральный закон «Об обязательном экземпляре документов» от 29 декабря 1994 года №77–ФЗ впервые ввёл понятие документа. Гражданский кодекс 1994 года в ст. 128 отнёс информацию и результаты интеллектуальной деятельности к объектам гражданских прав, а в статье 139 закрепил право на служебную или коммерческую тайну (статья отменена с 1 января 2008).

Тем не менее, система правовой защиты киберпреступлений без уголовно–правовых мер считалась несостоявшейся. Работу над проектом изменений в УК РСФСР вели Минюст РФ и Госправовое управление Президента. Подготовили два проекта, правильно определив родовой объект – преступления против общественной безопасности и порядка. Проекты мало отличались по составам, но юристы и ИТ–специалисты раскритиковали слабую стилистику и отсутствие чёткой терминологии. В связи с этим, была создана согласительная комиссия Госдумы.

С 1 января 1997 года в УК РФ вступила в силу глава 28, включившая три состава: ст. 272 (неправомерный доступ к компьютерной информации), ст. 273 (создание и распространение вредоносных программ), ст. 274 (нарушение

[1] Китайкина О. О. Российское законодательство об уголовной ответственности за преступления в сфере компьютерной информации: история и современность // Научный формат. – 2020. – №12(15). – С.20.

правил эксплуатации средств хранения, обработки или передачи информации). При совершении цифровых мошенничеств распространена квалификация по совокупности данных преступлений с иными составами, что позволяет полнее оценить общественную опасность деяния.

Важным этапом развития уголовного законодательства стало осознание того, что традиционная статья 159 УК РФ, предусматривающая ответственность за мошенничество, не в полной мере охватывает случаи хищений, совершаемых с использованием новых технологий. Законодатель пошел по пути не создания единого состава «кибермошенничества», а выделения отдельных, специальных составов.

Так, Федеральным законом от 29 ноября 2012 г. № 207–ФЗ Уголовный кодекс РФ был дополнен статьей 159.3 «Мошенничество с использованием электронных средств платежа» и статьей 159.6 «Мошенничество в сфере компьютерной информации».[1] Самостоятельные нормы о мошенничестве, совершаемом посредством сети Интернет, законодатель до настоящего времени не выделяет, квалифицируя такие деяния по общим или указанным специальным составам в зависимости от конкретного способа совершения преступления.

Тем самым российский законодатель избрал модель, при которой уголовная ответственность дифференцируется в зависимости от «предмета» или «способа» посягательства (электронные средства платежа или компьютерная информация), а не от среды совершения (цифровое пространство).

Параллельно с уголовным законом развивалось и общее регулирование. Доктрина информационной безопасности РФ (2000 г.) заложила основы государственной политики в данной сфере. В связи с ростом глобальных информационных систем 7 июля 2003 года принят Закон «О связи».

Существенные изменения уголовно–правовых норм последовали с Федеральным законом от 7 декабря 2011 г. № 420–ФЗ: в ст. 272 введён квалифицирующий признак корыстной заинтересованности, а ч. 3 ст. 273 дополнена ответственностью за создание и использование программ,

[1] О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации: Федеральный закон от 29.11.2012 №207-ФЗ (ред. от 03.07.2016) // Собрание законодательства РФ. – 2012. – № 49. – Ст. 6752.

предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования информации либо нейтрализации средств защиты.

5 декабря 2016 года утверждена новая Доктрина информационной безопасности. С 1 января 2018 года в УК ввели статью 274.1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации» – из–за высокой общественной опасности такого вреда. Статья отсылает к Федеральному закону № 187–ФЗ от 26 июля 2017 года.

9 мая 2017 года утверждена Стратегия развития информационного общества на 2017–2030 годы, где среди принципов – защита интересов граждан в информационной сфере, введены понятия «безопасного ПО», «индустриального интернета», «информационного пространства».

В настоящее время киберпреступность также не остается без внимания, реформы нормативно–правового регулирования продолжились.

В 2022 г. Федеральным законом от 14 июля № 260–ФЗ ввели статью 274.2 – ответственность за нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования сети «Интернет» и связи общего пользования в РФ.[1]

В 2024 г. принят Федеральный закон от 30 ноября № 421–ФЗ, дополнивший УК статьей 272.1. По ней наступает ответственность за незаконное использование, передачу, сбор или хранение компьютерной информации с персональными данными, а также за создание или обеспечение работы ресурсов для их незаконного хранения или распространения.[2]

15 декабря 2022 г. Пленум Верховного Суда РФ принял постановление «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации…». В нём разъяснены понятия уничтожения, копирования, нейтрализации средств защиты; термин «собственник или законный владелец» заменён на «обладатель информации». Компьютерная информация – любые сведения в виде электрических сигналов, а компьютерные устройства – любые электронные устройства для приёма, обработки, хранения и передачи информации.

---

[1] О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации: Федеральный закон от 14.07.2022 № 260-ФЗ (ред. от 14.07.2022) // Собрание законодательства РФ. – 2022. – № 29 (ч. II). – Ст. 5227.

[2] О внесении изменений в Уголовный кодекс Российской Федерации: Федеральный закон от 30.11.2024 № 421-ФЗ (ред. от 11.12.2024) // Собрание законодательства РФ. – 2022. – № 29 (ч. IV). – Ст. 7412.

Преступление по ст. 272 УК РФ окончено с момента наступления хотя бы одного последствия (уничтожение, блокирование, модификация, копирование) независимо от длительности доступа. Не образует состава использование вредоносной программы на своих устройствах либо с согласия собственника, если нет цели неправомерного доступа к охраняемой информации.[1]

1 апреля 2025 г. принят федеральный закон № 41–ФЗ «О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий…». [2]

Он вводит обязательную маркировку звонков от организаций; запрещает сотрудникам Банка России, госорганов, банков и операторов связи общаться с гражданами через иностранные мессенджеры; запрещает передачу SIM–карт третьим лицам (кроме членов семьи и близких родственников); даёт абоненту право отказаться от рассылок и массовых вызовов; позволяет гражданам установить запрет на заключение договоров связи без личного присутствия. Также закреплены меры против выдачи наличных без добровольного согласия клиента через банкоматы.

Таким образом, российское законодательство прошло путь от полного отсутствия норм до разветвлённой системы, включающей материальные составы (ст. 272–274.2 УК РФ), процессуальные и организационные механизмы. Компьютерная преступность – серьёзная угроза, ущерб от неё исчисляется миллиардами долларов, а сами преступления носят межгосударственный характер. Россия включилась в процесс криминализации позже западных стран, но сегодня обладает сопоставимым по строгости и охвату законодательством. При этом только уголовно–правового регулирования недостаточно, поскольку многие вопросы одновременно регулируются уголовным законом и связаны с разными сторонами информационных отношений.

[1] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 09.04.2026) // Собрание законодательства РФ. – 1996. – № 43. – Ст. 4190.

[2] О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий: Федеральный закон от 01.04.2025 № 41-ФЗ (ред. от 31.07.2025) // Собрание законодательства РФ. – 2022. – № 14. – Ст. 1574.

1.2 Понятие, признаки и характеристика мошенничества в цифровом пространстве

Актуальность обращения к понятию, признакам и характеристике мошенничества в цифровом пространстве в рамках настоящего исследования обусловлена стремительной трансформацией общественных отношений, опосредованных информационно–телекоммуникационными технологиями.

Ежегодный рост числа зарегистрированных преступлений, совершаемых с использованием сети Интернет, мобильной связи и электронных средств платежа, свидетельствует о том, что традиционные уголовно–правовые конструкции не всегда успевают адаптироваться к новым криминальным реалиям.[1]

По оценкам Statista's Market Insights, глобальный ущерб от киберпреступности, как ожидается, серьезно вырастет в ближайшие четыре года: с 9,22 трлн долларов в 2024 г. до 13,82 трлн к 2028 г. (Приложение А).[2]

Согласно официальным данным МВД России, за последние пять лет доля дистанционных хищений в общем массиве зарегистрированных преступлений против собственности увеличилась более чем в два раза, при этом значительную часть из них составляют именно мошеннические посягательства.

В этих условиях возникает объективная необходимость не только в уточнении законодательных дефиниций, но и в выработке доктринального подхода, позволяющего чётко отграничить цифровое мошенничество от смежных составов, а также определить его сущностные признаки.

Цифровое пространство как среда совершения преступления вносит качественные изменения в механизм обмана или злоупотребления доверием, что, в свою очередь, требует пересмотра некоторых элементов юридической

[1] Дрёмин А. А. Современное состояние и динамика преступности мошенничества с использованием электронных средств платежа в 2025 году // Вестник науки. – 2025. – № 6. – С. 73.
[2] Ущерб от киберпреступлений вырастет на треть за следующие 4 года: институт изучения мировых рынков. – URL: https://worldmarketstudies.ru/article/userb-ot-kiberprestuplenij-vyrastet-na-tret-za-sleduusie-4-goda/ (дата обращения: 02.05.2026).

характеристики состава.

Несмотря на наличие разъяснений Пленума Верховного Суда Российской Федерации и ряда специальных норм (ст. 159.3 и 159.6 УК РФ), правоприменительная практика сталкивается с трудностями при квалификации деяний, когда мошеннический обман реализуется посредством фишинговых рассылок, подмены телефонных номеров, создания поддельных мобильных приложений или использования криптовалют.[1]

Более того, дискуссионным остаётся вопрос о моменте окончания такого мошенничества, о возможности признания цифровых активов (например, внутриигровой валюты или криптовалюты) предметом преступления, а также о достаточности существующих признаков для отграничения мошенничества от неправомерного доступа к компьютерной информации, если последний выступает лишь способом хищения.

Переходя к рассмотрению понятия мошенничества в цифровом пространстве, необходимо отметить, что легальное определение мошенничества содержится в части первой ст. 159 УК РФ, где под ним понимается хищение чужого имущества или приобретение права на чужое имущество путём обмана или злоупотребления доверием. Данное определение является родовым для всех видов мошенничества, включая те, которые совершаются с использованием цифровых технологий.

В свою очередь, УКРФ содержит специальную норму – ст. 159.6 «Мошенничество в сфере компьютерной информации», которая определяет это деяние как хищение чужого имущества или приобретение права на чужое имущество путём ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно–телекоммуникационных сетей.[2]

---

[1] О судебной практике по делам о мошенничестве, присвоении и растрате: Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 (ред. от 15.12.2022) //Российская газета. – 2017. – № 280.

[2] Уголовный кодекс Российской Федерации: Федеральный закон от 13.06.1996 № 63-ФЗ (ред. от 09.04.2026) // Собрание законодательства РФ. – 1996. – № 43.– Ст. 2954.

Как видно из данного определения, ключевое отличие состоит в способе совершения: если в общей норме акцент сделан на обман или злоупотребление доверием, то в ста.159.6 – на техническое воздействие на компьютерную информацию и информационную инфраструктуру.

При этом в научной среде продолжается дискуссия относительно определения преступлений в сфере компьютерной информации и киберпреступности в целом. Различные исследователи предлагают свои формулировки.

Ряд учёных использует термин «компьютерные преступления», понимая под ним деяния, где машинная информация является предметом посягательства.

А. П. Кузнецова и соавторы акцентируют внимание на причинении вреда отношениям, обеспечивающим компьютерную безопасность.[1]

Существует также подход к разделению понятия на узкое (преступления, возможные только с использованием компьютера) и широкое (любое использование компьютера как объекта или инструмента преступления) толкование. Учёные используют разные термины для обозначения исследуемых деяний: «компьютерные преступления», «преступления против компьютерной информации», «преступления в сфере использования компьютерной информации».

При этом кибермошенничество в доктрине часто рассматривается как разновидность киберпреступности – сложного правового феномена, включающего различные формы противоправных действий, где информационно–коммуникационные технологии выступают инструментом или средой.

И. А. Кучерков определяет киберпреступность как преступность в информационном пространстве, моделируемом при помощи компьютера, где находятся сведения о лицах, предметах, фактах, событиях, явлениях и

[1] Кузнецова А. П. Позиция Пленума о квалификации мошенничества требует уточнения // Российская юстиция. – 2015. –№ 5. – С.69.

процессах.[1]

В. А. Номоконов полагает, что 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.[2]

Анализ приведённых подходов показывает, что кибермошенничество не тождественно мошенничеству в сфере компьютерной информации в узком смысле ст. 159.6 УК РФ, поскольку оно может быть реализовано не только путём технического вмешательства, но и через социальную инженерию, фишинг, подмену номера и иные способы, где воздействие на компьютерную информацию не является основным.[3]

В то же время общее определение мошенничества в цифровом пространстве, нуждается в уточнении с учётом доктринальных разработок.

Так, на основе анализа изложенных научных позиций, а также содержания ст.ст. 159 и 159.6 УК РФ, представляется возможным сформулировать авторское определение кибермошенничества (мошенничества в цифровом пространстве) как умышленного безвозмездного изъятия и (или) обращения чужого имущества или приобретения права на него, совершённого путём обмана или злоупотребления доверием, реализованных с использованием информационно–телекоммуникационных технологий, включая сеть Интернет, мобильную связь, электронные средства платежа, а также путём ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно–телекоммуникационных сетей, если такое вмешательство служит способом обмана или условием для хищения.

---

[1] Кучерков И. А. О понятии «киберпреступление» в законодательстве и научной доктрине // Информационное право. – 2019. – №10. – С.78.

[2] Номоконов В. А., Тропина Т. Л. Киберпреступность как новая криминальная угроза // Криминология интернет-пространства. – 2012. – №12. – С.45.

[3] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 09.04.2026) // Собрание законодательства РФ. – 1996. – № 25. – Ст. 2954.

Данное определение, в отличие от узкого понимания киберпреступности только как посягательств на компьютерную информацию, охватывает обе группы деяний: как те, где цифровые технологии выступают орудием обмана (звонки, фишинг, поддельные сайты), так и те, где хищение опосредовано прямым техническим вмешательством в работу компьютерных систем (ст. 159.6 УК РФ).

Такой подход соответствует широкому толкованию киберпреступности, поддерживаемому большинством современных исследователей, и позволяет унифицировать правоприменительную практику в условиях цифровой трансформации. Само же цифровое пространство, применительно к целям настоящей работы, понимается как среда, генерируемая и поддерживаемая информационно–коммуникационными технологиями, в которой осуществляется обмен данными, совершаются сделки, возникают и реализуются имущественные права, а также совершаются противоправные деяния, включая мошеннические.

Для более глубокого понимания сущности мошенничества в цифровом пространстве необходимо различать общие признаки, присущие любому хищению в форме мошенничества, и специальные, отражающие специфику цифровой среды.

К общим признакам относятся: противоправность (изъятие имущества без законного основания, выражающаяся в отсутствии права на чужие денежные средства, данные или цифровые активы); безвозмездность (собственник не получает эквивалентного возмещения, а символическая оплата, например 1 рубль, этого не меняет); корыстная цель (стремление к незаконной выгоде, нередко замаскированной под легальные действия вроде возврата налога или выигрыша); причинение ущерба собственнику (уменьшение наличных, списание безналичных средств, утрата криптовалюты или блокировка доступа к ценным цифровым аккаунтам).[1]

[1] Савельев Д. В. Уголовное право. Общая часть: учебник для вузов. – М.: Юрайт, 2025. – С. 34.

Помимо этих четырёх признаков, системообразующим для мошенничества является обман или злоупотребление доверием как специфический способ совершения преступления, который в цифровом пространстве приобретает новые черты.[1]

Обман как способ совершения преступления в цифровой среде может принимать различные формы: от прямого ложного сообщения (например, звонок от «сотрудника службы безопасности банка» с информацией о подозрительной операции) до создания полностью поддельной цифровой среды (фишинговый сайт, имитирующий портал государственных услуг, или поддельное мобильное приложение).[2]

При этом существенным признаком является то, что потерпевший добровольно, под влиянием заблуждения, совершает действия по передаче имущества или предоставлению доступа к нему. Именно добровольность отличает мошенничество от кражи, где имущество изымается без согласия собственника.

В цифровом пространстве добровольность может быть иллюзорной: жертва сама переводит деньги на счёт злоумышленника, сама сообщает код из SMS, сама устанавливает вредоносное программное обеспечение. Однако эта «добровольность» является вынужденной и основанной на ложных сведениях, что полностью соответствует конструкции мошеннического обмана.

Что касается злоупотребления доверием в цифровом пространстве, то оно встречается реже, но также имеет место. Например, если лицо, которому потерпевший доверил пароль от онлайн–банка для оплаты коммунальных услуг, использует этот пароль для перевода средств на свой счёт, то налицо злоупотребление доверием, реализованное с использованием цифровой технологии.

Специальные признаки мошенничества в цифровом пространстве

[1] Витвицкая С. С. Киберпреступления: понятие, классификация, международное противодействие // Правовой порядок и правовые ценности. – 2023. – № 1. – С. 126.

[2] О судебной практике по делам о мошенничестве, присвоении и растрате: Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 (ред. от 15.12.2022) //Российская газета. – 2017. – № 280.

включают в себя:

– использование информационно–телекоммуникационной сети (в том числе сети Интернет) как канала связи и как инструмента воздействия;

– дистанционный характер взаимодействия между преступником и потерпевшим (отсутствие непосредственного физического контакта);

– высокую степень латентности, обусловленную возможностью использования анонимных технологий (VPN, прокси–серверы, криптовалютные миксеры);

– трансграничный характер, когда действия по обману, изъятию имущества и получению выгоды могут совершаться в разных юрисдикциях;

– использование социальной инженерии как метода манипуляции сознанием, адаптированного под цифровые каналы связи;

– создание цифровых копий официальных сайтов, документов, приложений, визуально неотличимых от подлинных;

– применение автоматизированных систем (роботизированных обзвонов, чат–ботов) для массового воздействия на потенциальных жертв.[1]

Важно подчеркнуть, что наличие хотя бы одного из перечисленных специальных признаков позволяет говорить о цифровой природе мошенничества, хотя на практике они часто встречаются в совокупности.

Например, типичная схема «звонок из банка» включает в себя дистанционное взаимодействие (телефонная связь), использование социальной инженерии (легенда о подозрительной операции), часто – подмену номера, чтобы он совпадал с официальным номером банка, и в ряде случаев – последующий перевод денег через электронные средства платежа.

Анализ судебной практики показывает, что суды не всегда акцентируют внимание на цифровых признаках, ограничиваясь констатацией обмана и хищения. Однако для исследования важно зафиксировать, что именно

[1] Айнутдинова К. А. Виктимологические особенности киберпреступности в условиях цифровой трансформации общества: материалы национальной научно-практической конференции в 2-х частях / К. А. Айнутдинова. – Казань: ТИСБИ, 2022. – С.34.

совокупность общих и специальных признаков образует юридическую конструкцию мошенничества в цифровом пространстве как особого криминального феномена, требующего адекватного правового реагирования.

Характеристика состава мошенничества в цифровом пространстве предполагает последовательный анализ его элементов: объекта, объективной стороны, субъекта и субъективной стороны. Каждый из этих элементов в условиях цифровой трансформации приобретает определённую специфику, которая, однако, не отменяет общей логики построения состава преступления, закреплённой в теории уголовного права.[1]

Начнём с рассмотрения объекта преступления.

Родовым объектом для мошенничества в цифровом пространстве выступают отношения собственности, а видовым – отношения в сфере экономической деятельности. Непосредственным объектом является конкретная форма собственности (частная, государственная, муниципальная или иная), которой причиняется ущерб в результате хищения.

В цифровом пространстве объект не утрачивает своего материального или имущественного характера, однако появляются дополнительные объекты, которым может быть причинён вред. Речь идёт, в частности, о безопасности компьютерной информации, о праве на тайну переписки, телефонных переговоров и иных сообщений, о праве граждан на достоверную информацию. Поэтому в литературе иногда выделяют дополнительный объект мошенничества в цифровом пространстве – общественные отношения в сфере информационной безопасности.

Хотя уголовный закон прямо не называет информационную безопасность в качестве самостоятельного объекта при квалификации по статье 159 УК РФ, суды при назначении наказания учитывают, что преступление совершалось с использованием цифровых технологий, что

[1] Уторова Т. Н. Преступления в сфере информационной безопасности: учебное пособие. – Вологда: Северо-Западный ин-т (филиал) Ун-та им. О. Е. Кутафина (МГЮА), 2024. – С.35.

повышает общественную опасность.[1]

Следует также остановиться на предмете преступления, поскольку в цифровом пространстве он претерпевает существенные изменения. Предметом мошенничества, как следует из ст. 159 УК РФ, является чужое имущество или право на чужое имущество.

В традиционном понимании имущество – это вещи, включая деньги и ценные бумаги. Однако в цифровой среде появляются такие объекты, как электронные денежные средства (денежные средства, хранящиеся на банковских картах и в электронных кошельках), криптовалюта (биткоин, эфириум и иные цифровые валюты), цифровой рубль, а также внутриигровые ценности (скины, очки, игровая валюта, аккаунты).

Позиция Верховного Суда Российской Федерации по данному вопросу выражена в Постановлении Пленума № 48 от 30.11.2017 «О судебной практике по делам о мошенничестве, присвоении и растрате», где разъяснено, что предметом хищения могут быть безналичные денежные средства, в том числе электронные, при условии, что они являются средством платежа и имеют экономическую ценность.[2]

Что касается криптовалюты, то однозначной позиции до сих пор не сложилось, однако в судебной практике встречаются случаи признания криптовалюты имуществом, если она была приобретена за реальные деньги или может быть конвертирована в фиатные средства.

При этом хищение криптовалюты путём обмана (например, под видом предложения инвестиций в цифровые активы) квалифицируется как мошенничество по ст. 159 УК РФ, если доказан умысел на безвозмездное изъятие.

Сложнее обстоит дело с внутриигровыми предметами: здесь подходы разнятся, но тенденция такова, что если виртуальный предмет имеет реальную

[1] Уголовный кодекс Российской Федерации: Федеральный закон от 13.06.1996 № 63-ФЗ (ред. от 09.04.2026) // Собрание законодательства РФ. – 1996. – № 43. – Ст. 4190.

[2] О судебной практике по делам о мошенничестве, присвоении и растрате: Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 (ред. от 15.12.2022) //Российская газета. – 2017. – № 280.

рыночную стоимость и может быть продан (например, через площадки по торговле игровыми аккаунтами), то он признаётся имуществом.

Таким образом, предмет мошенничества в цифровом пространстве расширяется за счёт цифровых активов, что требует от правоприменителя каждый раз устанавливать их экономическую ценность и принадлежность к чужому имуществу.

Переходя к объективной стороне состава, следует отметить, что она выражается в деянии (действии или бездействии), последствиях и причинной связи между ними. Объективная сторона мошенничества в цифровом пространстве характеризуется активными действиями по обману или злоупотреблению доверием с использованием цифровых технологий. В отличие от традиционного мошенничества, где обман часто носит устный или письменный характер, в цифровом пространстве он может быть реализован путём:

– направления электронного письма с поддельного адреса (фишинг);

– создания сайта–двойника, внешне неотличимого от официального;

– подмены телефонного номера при звонке (спуфинг);

– распространения вредоносного программного обеспечения под видом легального;

– манипуляции с настройками мобильного приложения или браузера;

– использования чат–ботов для автоматического обмана.[1]

Кроме того, объективная сторона может выражаться в форме технического вмешательства, предусмотренного ст. 159.6 УК РФ: ввод, удаление, блокирование, модификация компьютерной информации либо иное вмешательство в функционирование средств хранения, обработки или

[1] Зуев С. В., Вехов В. Б. Расследование преступлений в сфере компьютерной информации и электронных средств платежа: учебник для вузов. – М.: Юрайт, 2026. – С.45.

передачи компьютерной информации или информационно–телекоммуникационных сетей.[1]

В таких случаях обман может отсутствовать как самостоятельный элемент, а хищение происходит за счёт того, что компьютерная система выдаёт ложный результат обработки данных (например, изменение баланса счёта путём внедрения вредоносного кода).

Важно подчеркнуть, что способ обмана должен быть направлен на то, чтобы ввести потерпевшего в заблуждение относительно обстоятельств, имеющих значение для передачи имущества.

Особого внимания заслуживает такой элемент объективной стороны, как время и место совершения преступления. В цифровом мошенничестве действия по обману и изъятию имущества могут быть разорваны во времени и пространстве: обман может быть совершён в одном регионе (например, звонок из колл–центра), а списание средств – в другом, при этом счёт получателя может быть открыт в третьем регионе или даже в другой стране. Это создаёт сложности для определения подследственности и подсудности, но не влияет на квалификацию.

По российскому уголовному праву местом совершения преступления признаётся место, где было совершено общественно опасное действие (или бездействие), независимо от места наступления последствий. Поэтому при звонке из Москвы и переводе денег из Новосибирска местом совершения преступления будет признана Москва, что иногда вызывает споры. В целом объективная сторона мошенничества в цифровом пространстве сохраняет все классические элементы, но наполняется новым содержанием за счёт цифровых способов обмана, технического вмешательства в компьютерную информацию и особенностей наступления последствий.

[1] Уголовный кодекс Российской Федерации: Федеральный закон от 13.06.1996 № 63-ФЗ (ред. от 09.04.2026) // Собрание законодательства РФ. – 1996. – № 43. – Ст. 4190.

Субъект мошенничества в цифровом пространстве, как общее правило, является общим – это физическое вменяемое лицо, достигшее возраста уголовной ответственности.

Согласно ч. 1 ст. 20 УК РФ, ответственность за мошенничество (ст. 159 УК РФ) наступает с 16 лет. Исключение составляют случаи, когда мошенничество совершено в составе группы лиц по предварительному сговору или организованной группы, что влияет на квалификацию, но не на возрастной ценз. В литературе обсуждается вопрос о необходимости понижения возраста ответственности за цифровое мошенничество до 14 лет, поскольку подростки активно используют интернет и социальные сети и нередко становятся как жертвами, так и исполнителями таких преступлений.[1]

Однако законодатель пока не поддержал эту инициативу, и для квалификации по ст. 159 УК РФ необходим возраст 16 лет. В то же время, если мошенничество в цифровом пространстве подпадает под признаки ст. 159.3 или 159.6 УК РФ, возрастной ценз также составляет 16 лет.

Важной особенностью субъекта цифрового мошенничества является то, что он не обязательно должен обладать специальными техническими знаниями.

Например, для того чтобы позвонить потерпевшему и представиться сотрудником банка, не требуется знаний в области программирования. Достаточно обладать элементарными навыками пользователя мобильной связи и социальной инженерии. Однако если мошенничество совершается с использованием вредоносного программного обеспечения, созданного самим преступником, либо с использованием специально изготовленных фишинговых сайтов, такие знания могут рассматриваться как квалифицирующий признак? Прямого указания в законе на это нет, однако на практике наличие специальных знаний может учитываться при индивидуализации наказания.

[1] Уголовный кодекс Российской Федерации: Федеральный закон от 13.06.1996 № 63-ФЗ (ред. от 09.04.2026) // Собрание законодательства РФ. – 1996. – № 43. – Ст. 4190.

Более сложным является вопрос о субъекте при совершении мошенничества через подставных лиц (дропперов). Дроппер – это лицо, которое за вознаграждение предоставляет свои банковские реквизиты для обналичивания похищенных средств, часто не зная о преступной схеме в полном объёме. Если дроппер осознаёт, что деньги получены преступным путём, и действует в интересах организаторов, он признаётся соучастником (как правило, пособником) мошенничества. Если же дроппер был введён в заблуждение (например, ему сказали, что это переводы от клиентов онлайн–казино), то он не является субъектом преступления.[1]

Таким образом, субъективная сторона действий каждого участника цифровой мошеннической схемы требует тщательного доказывания. Также следует упомянуть о возможности привлечения к ответственности юридических лиц за мошенничество в цифровом пространстве.

В российском уголовном праве юридическое лицо не может быть субъектом преступления, однако возможно применение мер уголовно–правового характера в отношении юридического лица (ст. 104.1 УК РФ) – конфискация имущества, полученного в результате преступления. Но само уголовное наказание (лишение свободы, штраф и т.д.) назначается только физическим лицам.

В целом субъект мошенничества в цифровом пространстве не имеет кардинальных отличий от общего субъекта мошенничества, за исключением того, что в условиях анонимности и трансграничности идентификация субъекта значительно затруднена, что влияет на раскрываемость, но не на юридическую конструкцию состава.

Наконец, рассмотрим субъективную сторону мошенничества в цифровом пространстве, которая характеризуется виной в форме прямого умысла, корыстной целью и, в некоторых случаях, специальными мотивами. Прямой умысел означает, что лицо осознаёт общественную опасность своих

[1] Петраков С. В. Раскрытие и расследование преступлений, совершаемых с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации: учебное пособие. – СПб.: Санкт-Петербургская академия Следственного комитета, 2021. – С.45.

действий (то есть понимает, что путём обмана или злоупотребления доверием с использованием цифровых технологий либо путём технического вмешательства в компьютерную информацию изымает чужое имущество), предвидит неизбежность или реальную возможность наступления общественно опасных последствий в виде причинения ущерба собственнику и желает их наступления.[1]

В цифровом пространстве умысел должен охватывать не только факт хищения, но и использование именно цифрового способа обмана или технического вмешательства. Если лицо, например, случайно получило доступ к чужому аккаунту и воспользовалось им без обмана, то умысел будет иным (возможно, кража).

Важным элементом субъективной стороны является корыстная цель – стремление извлечь материальную выгоду для себя или других лиц. В отличие от некоторых иных преступлений против собственности, где возможен временный характер изъятия (например, самоуправство), мошенничество предполагает именно окончательное обращение имущества в свою пользу или пользу третьих лиц.

В цифровом пространстве корыстная цель может проявляться в самых разных формах: от прямого получения денег на свой счёт до получения криптовалюты, скинов или иных цифровых активов, которые впоследствии продаются.

Помимо умысла и корыстной цели, в некоторых работах выделяют такой элемент субъективной стороны, как осознание лицом того, что оно действует в цифровом пространстве. Хотя прямо закон этого не требует, на практике это может иметь значение для отграничения от неосторожных деяний. Например, если лицо ошибочно полагает, что переводит деньги на благотворительный счёт, и не осознаёт обмана, то его действия не образуют состава мошенничества.

[1] Раменская В. С. Уголовное право. Уголовный процесс. Криминология: учебное пособие. – Екатеринбург: Уральский университет, 2023. – С. 56.

В отношении характеристики важно также указать на отсутствие в составе мошенничества в цифровом пространстве такого признака, как неосторожная форма вины. Мошенничество не может быть совершено по неосторожности, поскольку для него характерны целенаправленные действия по введению в заблуждение или техническому вмешательству.

При этом потерпевший может действовать неосторожно (например, не проверив адрес сайта), но это не влияет на вину преступника. Интересной особенностью цифрового мошенничества является то, что умысел может возникать в процессе совершения действий. Например, лицо начинает переписку с потерпевшим с законной целью (продажа товара), но затем, получив предоплату, решает не отправлять товар и использовать обман для получения всей суммы. В таких случаях умысел признаётся возникшим в момент принятия решения о хищении, и содеянное квалифицируется как мошенничество.

В целом субъективная сторона мошенничества в цифровом пространстве не имеет принципиальных отличий от субъективной стороны традиционного мошенничества, однако практика доказывания сталкивается с трудностями из–за анонимности и возможности использования подставных лиц, у которых может отсутствовать корыстный умысел.

Таким образом, проведённый анализ элементов состава преступления позволяет сделать вывод, что характеристика мошенничества в цифровом пространстве базируется на классической четырёхэлементной структуре, но с учётом цифровой специфики, которая проявляется прежде всего в объекте (дополнительный объект – информационная безопасность), предмете (цифровые активы), объективной стороне (цифровые способы обмана и техническое вмешательство в компьютерную информацию) и в некоторых особенностях субъекта (возможность участия лиц без специальных знаний, проблема идентификации). Эта характеристика имеет не только теоретическое, но и практическое значение, поскольку правильная квалификация деяния напрямую зависит от установления всех признаков

состава применительно к конкретным обстоятельствам, опосредованным цифровыми технологиями.

2 Криминологическая характеристика и региональные особенности цифрового мошенничества

2.1 Криминологическая характеристика лиц, совершающих киберпреступления и их жертв

Обращаясь к вопросу о понятии и структуре личности киберпреступника, следует отметить, что личность преступника в криминологии традиционно понимается как совокупность социально значимых негативных свойств, сформировавшихся в процессе взаимодействия индивида с окружающей средой и ставших детерминантой совершения преступления. Применительно к сфере киберпреступности это определение приобретает ряд специфических черт.

Ключевое отличие личности киберпреступника от так называемого «традиционного» преступника заключается в том, что его противоправная деятельность, как правило, не предполагает прямого физического контакта с жертвой, осуществляется дистанционно и зачастую требует высокого уровня технической подготовки.[1]

Более того, значительная часть киберпреступников, особенно на начальных этапах своей деятельности, не осознают в полной мере общественную опасность своих действий, воспринимая их как своеобразную «интеллектуальную игру» или способ самоутверждения в виртуальной среде.

В структуре личности киберпреступника можно выделить три основных компонента: социально–демографический (пол, возраст, образование, род занятий), нравственно–психологический (система ценностей, мотивы, психологические особенности) и уголовно–правовой (специфика совершаемых деяний, роль в группе, наличие судимостей). Именно интеграция этих компонентов позволяет составить полноценный

[1] Раменская В. С. Уголовное право. Уголовный процесс. Криминология: учебное пособие. – Екатеринбург: Уральский университет, 2023. – С. 70.

криминологический портрет.

Анализ социально–демографических признаков киберпреступников, основанный на данных судебной статистики и результатах криминологических исследований за последние несколько лет, позволяет выявить устойчивые тенденции. Прежде всего, обращает на себя внимание ярко выраженный гендерный перекос: подавляющее большинство лиц, осужденных за совершение киберпреступлений и мошенничеств с использованием информационно–телекоммуникационных технологий, составляют мужчины.[1]

По данным различных источников, включая статистику Судебного департамента при Верховном Суде РФ и исследования Университета прокуратуры РФ, доля мужчин среди осужденных стабильно держится на уровне 80–85%.

Например, согласно сводным данным за 2021–2023 г., удельный вес мужчин среди осужденных по статьям о мошенничестве с использованием информационно–телекоммуникационных технологий превышает 84%, тогда как женщины составляют около 15–16%.

Вместе с тем наблюдается и постепенное увеличение доли женщин, привлекаемых к ответственности за пособничество в таких преступлениях, особенно в части, касающейся обналичивания денежных средств или поиска «дропов» (подставных лиц для вывода денег), что может свидетельствовать о феминизации данного сегмента преступности.

Возрастная структура киберпреступников также имеет выраженную специфику. Наибольшую криминальную активность в сфере киберпреступлений проявляют лица в возрасте от 18 до 29 лет.[2]

В структуре судимости за мошенничество с использованием информационно–коммуникационных технологий доля этой возрастной

[1] Белевитина Ю. В. Криминологический портрет личности киберпреступника в современной России // Инновационная наук». – 2022. – № 12-2. – С. 61.
[2] Ян А. С. Киберпреступность: особенности, развитие и мотивы киберпреступности // Вестник науки. – 2025. – № 10 (91). – С.434.

группы составляет около 55–58%. Это период, когда, с одной стороны, человек уже обладает достаточным уровнем цифровой грамотности и техническими навыками, а с другой – еще не имеет устойчивых социальных связей, стабильного дохода и сформированного правосознания.

Вторую по величине группу (примерно 33–35%) образуют лица в возрасте 30–49 лет. Интересно, что в сегменте преступлений, непосредственно связанных с неправомерным доступом к компьютерной информации (статья 272 УК РФ), возрастной профиль смещается в сторону еще более молодых лиц: около половины осужденных по этим составам находятся в возрасте 18–24 лет. Это подтверждает тезис о том, что наиболее сложные с технической точки зрения кибератаки требуют знаний, полученных в рамках современного образования, и чаще совершаются молодыми людьми. [1]

Доля несовершеннолетних среди осужденных за киберпреступления составляет около 7%, что является весьма значимым показателем, указывающим на раннюю вовлеченность подростков в противоправную деятельность в цифровой среде, зачастую под влиянием более взрослых организаторов. Лица старше 50 лет среди киберпреступников встречаются относительно редко, что объясняется, как правило, меньшей технической подготовкой и иной структурой мотивации.

Уровень образования киберпреступников – еще один важный индикатор. Вопреки распространенному стереотипу о «хакерах–вундеркиндах» с элитным техническим образованием, реальная картина более дифференцирована. Среди всех осужденных за киберпреступления и кибермошенничество примерно две трети имеют среднее или среднее специальное образование.

Вместе с тем, если рассматривать отдельно группу лиц, осужденных за преступления, предусмотренные главой 28 УК РФ («Преступления в сфере компьютерной информации»), то здесь доля лиц с высшим профессиональным

[1] Муллаярова П. А. Психологический портрет киберпреступника // Международный журнал гуманитарных и естественных наук. – 2021. – №56. – С.116.

образованием возрастает до одной трети, что существенно выше, чем в среднем по массиву уголовных дел. Это указывает на то, что для совершения деяний, связанных с созданием вредоносного программного обеспечения, взломом систем защиты или несанкционированным доступом к базам данных, требуются более глубокие специальные знания.[1]

В сфере же массового кибермошенничества, основанного на методах социальной инженерии, высокий уровень формального образования не является обязательным условием – здесь на первый план выходят коммуникативные навыки и психологическая подготовка.

Обращает на себя внимание высокий уровень криминальной активности лиц, не имеющих постоянного источника дохода и занятости. Практически половина осужденных за киберпреступления относились к категории неработающих и не учащихся. Это указывает на то, что для значительной части киберпреступников противоправная деятельность становится основным или существенным источником существования.

При этом около 20% осужденных, напротив, имели официальное место работы и использовали для совершения преступлений служебное положение, доступ к корпоративным сетям и базам данных. Такие «инсайдеры» представляют собой особо опасную категорию, поскольку обладают легитимным доступом к охраняемой информации и могут длительное время оставаться незамеченными. В социально–демографическом портрете киберпреступника также важно отметить высокий уровень рецидива: по имеющимся данным, около 38–40% осужденных имели неснятую или непогашенную судимость на момент совершения нового преступления, что говорит о стойкости криминальной установки и недостаточной эффективности существующих мер исправительного воздействия в этой сфере.

Переходя к уголовно–правовой и криминологической характеристике,

[1] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 09.04.2026) // Собрание законодательства РФ. – 1996. – № 43. – Ст. 4190.

или типологии, киберпреступников, необходимо отметить, что их классификация может строиться по нескольким основаниям. Прежде всего, по характеру преступной мотивации можно выделить следующие основные типы.

Корыстный тип – это самая многочисленная и распространенная категория. Действия таких преступников направлены на получение прямой финансовой выгоды. Сюда относятся кибермошенники, использующие методы социальной инженерии, создатели и распространители программ–вымогателей (ransomware), участники кардинговых схем (торговля данными банковских карт), а также организаторы криптоджекинга – скрытого майнинга криптовалюты на вычислительных мощностях жертв.

Второй тип – идеологически мотивированные преступники, или хактивисты. Их деятельность направлена не на личное обогащение, а на достижение политических, социальных или идеологических целей. Это могут быть атаки на государственные учреждения, публикация компрометирующих материалов (так называемый «доксинг»), дефейс (подмена контента) веб–сайтов, DDoS–атаки с целью дестабилизации работы сервисов. В 2024–2025 годах активность хактивистов остается на высоком уровне, хотя их доля в общем массиве киберпреступлений уступает корыстной.

Третий тип – деструктивные и игровые преступники, движимые желанием самоутвердиться, проверить свои навыки или просто «навредить ради вреда». Они часто не имеют четкой финансовой или политической цели, их действия могут быть направлены на удаление данных, блокировку серверов, распространение вирусов–«вандалов». К этому же типу можно отнести и так называемых «скрипткиддис» (script kiddies) – людей, не обладающих глубокими техническими познаниями, но использующих готовые скрипты и программы для атак с целью развлечения или самоутверждения в глазах сверстников.

Четвертый тип – преступники, действующие в рамках государственного заказа или промышленного шпионажа. Они обладают высоким

профессионализмом, финансируются из значительных источников и нацелены на хищение коммерческой тайны, интеллектуальной собственности, секретных данных. Такие APT–группы (Advanced Persistent Threat – угроза постоянного характера) действуют крайне скрытно и методично.[1]

По степени организации выделяют преступников–одиночек, действующих самостоятельно и отличающихся эгоцентризмом, а также групповые формирования: простые группы без иерархии и организованные группы с чётким разделением ролей (организаторы, технические специалисты, операторы, вспомогательный персонал). Согласно статистике, около 23% осуждённых совершают киберпреступления в составе группы по предварительному сговору и ещё примерно столько же – в составе организованной группы, то есть почти половина всех таких преступлений совершается в форме соучастия. Высокий уровень организации позволяет действовать в промышленных масштабах.

Психологические и нравственно–психологические особенности киберпреступников представляют собой отдельный важный аспект криминологической характеристики. Киберпространство создает уникальную среду, которая во многом нивелирует традиционные механизмы социального контроля и способствует формированию специфических личностных деформаций.

Одной из ключевых черт, выделяемых исследователями, является так называемый «синдром анонимности» – уверенность в собственной неуязвимости и безнаказанности, возникающая благодаря возможности скрывать свою истинную личность за цифровыми псевдонимами, использовать прокси–серверы, VPN и другие средства анонимизации. Эта иллюзия безнаказанности, подкрепляемая высоким уровнем латентности киберпреступлений, существенно снижает внутренние барьеры, удерживающие человека от совершения противоправных действий.

[1] Айнутдинова К. А. Виктимологические особенности киберпреступности в условиях цифровой трансформации общества: материалы национальной научно-практической конференции в 2-х частях. – Казань: ТИСБИ, 2022. – С.35.

Для многих киберпреступников характерна также низкая эмпатия – неспособность или нежелание сопереживать жертве, которая воспринимается не как живой человек с его чувствами и потерями, а как абстрактный «аккаунт», «банковская карта» или «кошелек». Этот эффект дегуманизации усиливается дистанционным характером взаимодействия. Социальная отчужденность – еще одна распространенная черта. Многие киберпреступники, особенно на начальных этапах своей деятельности, испытывают трудности в реальном социальном взаимодействии, имеют заниженную самооценку, которую компенсируют в виртуальной среде, где их технические навыки приносят признание и авторитет. Исследования показывают, что для них характерна высокая импульсивность, слабая терпимость к фрустрации и склонность к агрессивным реакциям, но при этом они могут быть крайне хладнокровны и методичны при планировании атак.

Нравственно–психологический облик киберпреступника нередко характеризуется искаженным пониманием справедливости (убеждение, что «взламывать богатых и корпорации – это не воровство, а перераспределение») и сниженным чувством ответственности за последствия своих действий. В то же время многие из них демонстрируют высокий интеллектуальный потенциал, развитое логическое мышление и способность к длительному концентрации внимания.

Любопытно, что сотрудники Управления по организации борьбы с противоправным использованием информационно–коммуникационных технологий МВД РФ отмечают у кибермошенников такие черты, как нарциссизм, уверенность в своем превосходстве над жертвами, а также умение играть на эмоциях, используя либо агрессивный, либо, напротив, «слащавый» стиль общения. Слабые стороны таких преступников – боязнь уточняющих вопросов и проверки информации; столкнувшись с уверенным и осведомленным собеседником, они, как правило, теряют интерес и прекращают коммуникацию.

Вторая ключевая фигура криминологического анализа – жертва

киберпреступлений. Понятие и криминологическая характеристика жертв киберпреступлений базируются на теоретическом фундаменте – учения о жертве преступления.

В широком смысле под жертвой киберпреступления понимается физическое или юридическое лицо, которому в результате противоправных действий, совершенных с использованием информационно–телекоммуникационных технологий или в киберпространстве, причинен моральный, физический или имущественный вред. Специфика кибержертвы заключается в том, что ее виктимность (предрасположенность стать жертвой) во многом детерминирована не только личностными качествами, но и цифровым поведением, уровнем технической грамотности, а также самой средой, в которой происходит взаимодействие.

Жертвой киберпреступления может стать любой пользователь, но виктимность повышают: активное использование онлайн–банкинга, размещение личных данных в открытом доступе, низкая цифровая гигиена, доверчивость и неосведомлённость о схемах мошенников. В отличие от традиционной преступности, в киберпространстве между жертвой и преступником возможна огромная дистанция, что делает виктимологическую профилактику сложной, но крайне необходимой. По типу посягательства выделяют жертв кибермошенничества (самостоятельно перевели деньги или сообщили данные карт), кражи персональных данных (оформление кредитов и т.п.), кибербуллинга и домогательств (дети, подростки и взрослые), вымогательства (после заражения шифровальщиком), а также неправомерного доступа к аккаунтам (взлом страниц на «Госуслугах», в соцсетях).[1]

По характеру поведения в момент совершения преступления можно выделить несколько типов жертв.

Пассивные жертвы – те, кто не оказывает сопротивления, не пытается проверить информацию и подчиняется требованиям мошенника, что часто

[1] Айнутдинова К. А. Виктимологические особенности киберпреступности в условиях цифровой трансформации общества: материалы национальной научно-практической конференции в 2-х частях. – Казань: ТИСБИ, 2022. – С.37.

связано с состоянием растерянности, страха или внушенной срочности.

Активные, но некритичные жертвы – они совершают активные действия (переводят деньги, сообщают коды из СМС, устанавливают программы удаленного доступа), но при этом не осознают преступный характер требований, полностью доверяя легенде мошенника.

Провоцирующие жертвы – своим поведением (например, публичное хвастовство крупными суммами на счетах, размещение сканов документов в открытом доступе, грубость и оскорбления в адрес других пользователей) они сознательно или неосознанно привлекают внимание преступников и облегчают реализацию преступного умысла.

И наконец, критически настроенные жертвы – они, столкнувшись с подозрительной активностью, прерывают контакт, самостоятельно проверяют информацию (например, перезванивают в банк по официальному номеру) и тем самым предотвращают преступление.

По степени вовлеченности в ситуацию также выделяют нейтральных жертв (поведение не способствует и не препятствует преступлению), аккомодирующих жертв (своей наивностью, доверчивостью, неопытностью создают благоприятные условия для преступника) и противодействующих жертв (проявляют мнительность, подозрительность, активно проверяют информацию).

Социально–демографический портрет жертвы киберпреступлений, особенно наиболее распространенных составов – кибермошенничества и неправомерного доступа к аккаунтам, может быть реконструирован на основе данных Банка России, МВД РФ и результатов независимых опросов. Долгое время считалось, что основные жертвы – это пожилые люди, недостаточно владеющие современными технологиями. Однако данные 2023–2025 г. демонстрируют более сложную картину.

Согласно ежегодному опросу Банка России, в 2024 г. типичный портрет жертвы кибермошенников выглядел следующим образом: это работающая женщина в возрасте 25–44 лет (36,1% от общего числа пострадавших),

проживающая в городе, имеющая средний уровень дохода и образования, активно пользующаяся банковскими услугами и социальными сетями. Вторую по величине группу составили лица 45–64 лет (27,5%), а третью – граждане старше 65 лет (16,6%), причем последняя группа демонстрирует устойчивую тенденцию к росту.

Таким образом, происходит смещение «зоны риска» в сторону экономически активного населения среднего возраста. Любопытно, что если в 2023 году доля женщин среди пострадавших была выше доли мужчин на 11 процентных пунктов, то в 2024 г. этот разрыв сократился до 5,2 процентных пункта (57% женщин против 43% мужчин). Это может свидетельствовать как о росте женской финансовой активности, так и о том, что мошеннические схемы становятся более универсальными и нацеленными на любую аудиторию.

При этом уровень образования жертв варьируется, но значительная часть пострадавших имеет среднее специальное или среднее образование. Важный вывод, который делает управляющий Федеральным фондом по защите прав вкладчиков и акционеров Марат Сафиулин: «усредненный» портрет жертвы весьма условен, поскольку мошеннические схемы – это узкоспециализированные «продукты», ориентированные на конкретные аудитории. Для пенсионеров создается одна легенда (например, «сын попал в ДТП», «компенсация за лекарства»), для работающих граждан – другая («звонок из службы безопасности банка», «руководитель просит перевести деньги»), для студентов – третья («выигрыш в конкурсе», «предложение легкого заработка»). Поэтому говорить об одной–единственной «группе риска» некорректно – в зависимости от схемы жертвой может оказаться любой человек.[1]

Виктимологический аспект включает анализ поведения жертвы на трёх стадиях. До преступления – это цифровые привычки, повышающие

[1] НТВ и научный сотрудник Лаборатории финансовой грамотности ЭФ Марат Сафиулин о финансовой пирамиде QBF. – URL: https://www.econ.msu.ru/about/comments/Article (дата обращения: 02.05.2026).

виктимность: слабые пароли, переход по ссылкам из подозрительных сообщений, скачивание нелицензионного ПО, избыточное раскрытие личных данных, необдуманное согласие на доступ приложений к функциям устройства. Многие пострадавшие позже признают, что знали о схемах мошенников, но не придали этому значения. В момент преступления мошенники через социальную инженерию создают аффект (страх, жадность), используют ложную срочность, ссылки на авторитет или родственные чувства. Критическое мышление подавляется, жертва переводит деньги, называет коды, устанавливает приложения удалённого доступа. Согласно данным ЦБ РФ, 84,4% не поддались на уловки, но 15,6% совершили действия под влиянием, из них около 9% потеряли деньги. Поведение после преступления также важно в виктимологическом плане.

К сожалению, многие жертвы не обращаются в правоохранительные органы. Причины могут быть разными: стыд за собственную доверчивость и неосмотрительность, неверие в то, что преступников найдут и деньги вернут, страх перед оглаской или бюрократическими сложностями, а также непонимание того, что произошло (особенно у пожилых людей).

По данным опросов, значительная часть пострадавших никуда не обращаются, особенно если сумма ущерба невелика (до 20 тыс. рублей). Те же, кто обращается, чаще всего идут в банк или в полицию. Важно, что с июля 2024 года в России действует закон, обязывающий банки возмещать клиентам похищенные деньги, если перевод на подозрительный счет из базы данных Банка России не был приостановлен на два дня. Однако на практике подавляющее большинство граждан переводят деньги сами, и доказать, что банк должен был предотвратить операцию, бывает сложно.

Наконец, важнейшим аспектом криминологического анализа является взаимосвязь между личностью преступника и личностью жертвы в киберпространстве. В отличие от традиционной преступности, где нередко прослеживается прямая связь (например, жертва и преступник могут быть знакомы, находиться в конфликтных отношениях или, напротив, жертва своим

вызывающим поведением провоцирует нападение), в киберпространстве эта связь имеет опосредованный, дистанционный характер. Виктимологическая встреча в цифровой среде проявляется в нескольких аспектах. Во–первых, это целенаправленный поиск или создание ловушек преступником в соцсетях, мессенджерах, на маркетплейсах и других платформах. Во–вторых, это информационный разрыв: преступник обладает гораздо более глубокими знаниями технологий и методов обмана, что позволяет ему управлять поведением жертвы. В–третьих, это психологическая подстройка: мошенник быстро оценивает психотип жертвы и адаптирует свой стиль общения – от агрессии до участливости.

Таким образом, жертва в киберпространстве – это не просто случайный объект, а элемент виктимной ситуации, которая может быть создана как действиями преступника, так и неосторожным или провоцирующим поведением самого потерпевшего. Понимание этой двусторонней связи имеет ключевое значение для профилактики: необходимо не только совершенствовать технические средства защиты информации и повышать эффективность работы правоохранительных органов, но и системно формировать у населения культуру цифровой гигиены, критическое мышление и устойчивость к методам социальной инженерии. Обучение граждан распознавать признаки мошенничества, проверять информацию, не поддаваться на создание ложной срочности и прерывать сомнительные контакты – это столь же важная часть противодействия киберпреступности, как и разработка антивирусных программ.

Подводя итог всему вышесказанному, можно сделать следующие выводы. Киберпреступность – сложное динамичное явление; портреты преступника и жертвы отличаются от традиционных. Типичный киберпреступник – мужчина 18–29 лет, с техническим образованием, высокой квалификацией или развитыми навыками социальной инженерии, корыстной мотивацией, низкой эмпатией и правовым нигилизмом.

Почти половина действуют в организованных группах, многие имеют

судимости. Жертва – уже не только пенсионер, а чаще работающая женщина 25–44 лет, активный пользователь цифровых сервисов, но с недостаточной цифровой грамотностью и критическим мышлением. Ключевой фактор виктимизации – доверие к авторитетным легендам и неспособность противостоять давлению через эффект срочности.

Взаимосвязь строится на информационном неравенстве и манипуляции. Профилактика должна быть двунаправленной: технико–правовые меры против преступников (разрушение групп, борьба с рецидивом) и активное виктимологическое просвещение населения (цифровая гигиена, психологическая устойчивость, информирование о схемах). Только комплексный подход снизит уровень киберпреступности и её социальные последствия.

2.2 Анализ состояния и динамики кибермошенничества в Пензенской области

В условиях стремительной цифровизации всех сфер общественной жизни, а также роста числа дистанционных способов совершения преступлений, изучение региональной специфики кибермошенничества приобретает особое значение.

Анализ общероссийской статистики позволяет выявить основные тренды развития кибермошенничества. Согласно официальным данным МВД России, динамика числа зарегистрированных мошенничеств, предусмотренных статьями 159–159.6 УК РФ, за последние три года имела разнонаправленный характер. В 2023 г. было зафиксировано 353 201 преступление данной категории, в 2024 г. наблюдался рост до 380 344 преступлений. Однако уже в 2025 г. наметилась тенденция к снижению: количество зарегистрированных мошенничеств сократилось до 348 035 (Приложение Б).

Таким образом, пик регистрации мошенничеств пришелся на 2024 г.,

после чего последовало снижение показателей в 2025 г. Это свидетельствует как о возможной стабилизации криминогенной обстановки в сфере цифровых технологий, так и об адаптации правоохранительной системы к новым вызовам. Вместе с тем абсолютные цифры остаются крайне высокими, что подтверждает сохраняющуюся общественную опасность данного вида преступлений.[1]

В этом контексте Пензенская область, являясь типичным субъектом Приволжского федерального округа с сочетанием городского и сельского населения, развитой финансовой инфраструктурой и высокой долей пожилых граждан, демонстрирует динамику, во многом отражающую общероссийские тренды, но при этом обладающую рядом уникальных характеристик. Так, согласно официальным данным Министерства внутренних дел Российской Федерации (ФКУ «Главный информационно–аналитический центр»), по итогам января – декабря 2025 г. удельный вес преступлений, совершённых с использованием информационно–телекоммуникационных технологий или в сфере компьютерной информации, в общей структуре преступности по Пензенской области составил 47,9%.

Данный показатель позволяет отнести регион к числу субъектов Российской Федерации с наибольшим удельным весом рассматриваемых деяний, что свидетельствует о высокой степени цифровизации преступной активности.

Далее обратимся к общей характеристике киберпреступности в Пензенской области за анализируемый период.

Данные официальной статистики свидетельствуют о том, что проблема дистанционных хищений и иных противоправных деяний, совершаемых с использованием информационно–телекоммуникационных технологий, сохраняет высокую степень общественной опасности.

В 2023 году на территории региона было зарегистрировано 5 169

[1] Состояние преступности в России за январь – декабрь 2025 г. – URL: https://мвд.рф/reports/item/77848182// (дата обращения: 02.05.2026).

преступлений, совершенных с использованием ИТ–технологий. При этом важно отметить, что уже в тот период доля таких правонарушений в общей структуре преступности составила 47,8%, что указывало на фактическое доминирование киберпреступности над традиционными видами криминала.[1]

Существенное влияние на состояние региональной преступности в 2023 г. оказал резкий рост количества зарегистрированных фактов неправомерного доступа к компьютерной информации, который увеличился на 414,9 процента по сравнению с предыдущим периодом – с 443 до 2 281 случая. Одновременно с этим наблюдался прирост числа мошенничеств с использованием ИТ–технологий на 13,3 процента (с 2 422 до 2 743). Такая динамика позволяла говорить о качественном изменении криминальной среды: злоумышленники активно осваивали новые способы взлома учетных записей, фишинговые атаки и методы социальной инженерии, что напрямую отражалось на статистике.

В 2024 г. количество киберпреступлений в Пензенской области достигло максимального за рассматриваемый период значения – 6 916 фактов. По сравнению с 2023 г. рост составил 33,8 процента, что является весьма значительным показателем даже на фоне общероссийских тенденций. Доля ИТ–преступлений в общем массиве зарегистрированных деяний сохранилась на уровне 47,8 процента.[2]

Такой скачок был обусловлен несколькими факторами.

Во–первых, продолжала расти активность мошеннических колл–центров, как действующих с территории России, так и из–за рубежа.

Во–вторых, наблюдалось дальнейшее увеличение числа эпизодов неправомерного доступа к компьютерной информации, хотя и не такими темпами, как в 2023 г.

В–третьих, сказалось повышение выявляемости данных преступлений:

---

[1] Информация о состоянии оперативной обстановки и результатов работы органов и подразделений внутренних дел Пензенской области за 2025 год. – URL: https://58.мвд.рф/document/61495918 (дата обращения: 07.05.2026).

[2] В Пензенской области растет число киберпреступлений и мошенничеств. – URL: https://stolica58.ru/news/obcshestvo/v-penzenskoj (дата обращения: 02.05.2026).

правоохранительные органы стали лучше регистрировать факты кибермошенничества благодаря налаженному взаимодействию с банками и операторами связи.

Тем не менее, именно 2024 г. стал пиковым по абсолютному числу противоправных деяний рассматриваемой категории, что вызвало серьезную обеспокоенность как у региональных властей, так и у федерального центра.

В 2025 г. ситуация начала меняться в лучшую сторону. По итогам двенадцати месяцев было зарегистрировано 5 317 киберпреступлений, что на 23,1 процента меньше, чем в 2024 г.[1]

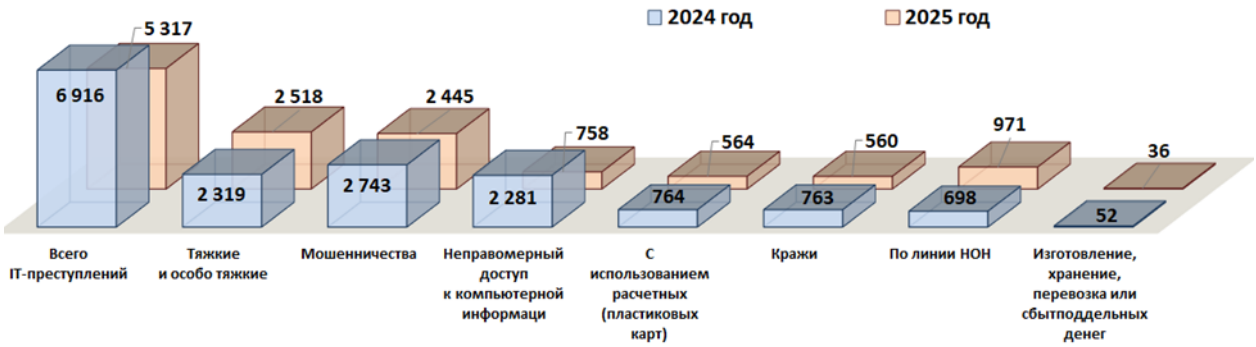


Рисунок 1 – Анализ показателей киберпреступлений в Пензенской области 2024–2025 гг.

При этом доля таких преступлений в общей структуре криминала незначительно снизилась до 47,9 процента. Важно подчеркнуть, что темпы снижения в Пензенской области оказались выше, чем в среднем по Приволжскому федеральному округу (минус 13,8 процента) и по России в целом (минус 11,8 процента). Это позволяет говорить о том, что комплекс мер, принятых на региональном уровне, дал положительный эффект.

По данным, озвученным на межведомственном совещании в прокуратуре Пензенской области 26 июня 2025 г., за первые пять месяцев года

[1] Информация о состоянии оперативной обстановки в Пензенской области за январь – декабрь 2025 г. – URL: https://58.мвд.рф/document/61495918 (дата обращения: 07.05.2026).

количество киберпреступлений сократилось на 24 процента по сравнению с аналогичным периодом прошлого года, однако они по–прежнему составляли 45 процентов от всех зарегистрированных преступлений.

В целом за 2025 г. правоохранительными органами предварительно расследованы уголовные дела по 1 021 преступлению, совершенному с использованием информационно–телекоммуникационных технологий. Особого внимания заслуживает тот факт, что общее количество зарегистрированных противоправных деяний данной категории в 2025 г. составило 4 894 (по данным декабрьского заседания рабочей группы), что также подтверждает тенденцию к снижению. Удельный вес киберпреступлений в этот период достиг 47 процентов.[1]

Далее рассмотрим динамику первых месяцев 2026 г. Согласно официальным данным, в январе и феврале 2026 г. количество ИТ–преступлений сократилось на 26 процентов по сравнению с аналогичным периодом 2025 г. – с 833 до 618 случаев. Доля таких правонарушений в общей структуре преступности снизилась до 39 процентов.

При этом важно учитывать, что данные за два месяца не всегда информативны для годовых выводов, однако столь устойчивое снижение (24–26 процентов на протяжении 2025 и начала 2026 г.) позволяет предположить наличие системных факторов, влияющих на криминогенную обстановку в сфере кибермошенничества.

Среди таких факторов, как будет показано далее, можно назвать как совершенствование работы правоохранительных органов и банковской системы, так и отдельные организационные меры, включая ограничение мобильного интернета в определенные периоды.

Таким образом, общая характеристика киберпреступности в Пензенской области свидетельствует о переходе от фазы активного роста (2023–2024 г.г.) к фазе стабилизации и снижения (2025–2026 годы), однако при сохранении

[1] Основные сведения о работе прокуратуры Пензенской области за 12 месяцев 2025 года. – URL: https://epp.genproc.gov.ru/ru/proc_58/activity/statistics/office/result/e8389158/ (дата обращения: 07.05.2026).

высокой доли таких преступлений в общем массиве криминала.

Переходя к анализу основных видов кибермошенничества в регионе, необходимо отметить, что структура ИТ–преступлений в Пензенской области является достаточно типичной для российских регионов, но имеет и свои особенности.

В 2025 г. наибольшую долю в массиве киберпреступлений составили мошенничества – 46%, что в абсолютных цифрах соответствует примерно 2 445 фактам. На втором месте оказался незаконный оборот наркотических средств с использованием ИТ–технологий – 18,3 процента (971 случай). Третью позицию занял неправомерный доступ к компьютерной информации – 14,3 процента (758 фактов), а четвертую – кражи чужого имущества, совершенные с применением информационно–телекоммуникационных технологий, – 10,5 процента (560 случаев).

Такое распределение показывает, что мошенничество остается основным и наиболее массовым видом киберпреступлений в регионе. При этом важно различать внутри самой категории мошенничества различные подвиды, поскольку от этого зависит выбор методов профилактики и расследования.

Наиболее распространенным видом остается телефонное мошенничество, в рамках которого злоумышленники звонят гражданам, представляясь сотрудниками банков, правоохранительных органов, сотовых операторов или иных организаций. Как следует из выступлений начальника отдела по борьбе с противоправным использованием ИКТ УМВД России по Пензенской области Романа Сальникова, типичными схемами являются: сообщение о попытке несанкционированного списания средств со счета и необходимости перевода денег на «безопасный счет»; информация о том, что родственник попал в беду и требуется срочный перевод денег для решения вопроса; звонок от лжесотрудника портала «Госуслуги» с требованием

сообщить код из SMS для восстановления доступа.[1]

В 2025–2026 г.г. получили распространение также комбинированные схемы, когда мошенники сначала взламывают аккаунт в мессенджере, а затем от имени владельца аккаунта рассылают просьбы о займе денег, подкрепляя их голосовыми сообщениями, сгенерированными с помощью нейросетей или записанными ранее.[2]

По данным Министерства общественной безопасности и обеспечения деятельности мировых судей Пензенской области, злоумышленники научились изучать переписку в мессенджерах и использовать голосовые сообщения для придания правдоподобия своим действиям, в связи с чем гражданам рекомендуется удалять голосовые сообщения из чатов после прослушивания и проверять любую финансовую информацию через дополнительные каналы связи.

Значительную долю составляют также мошенничества на сайтах бесплатных объявлений, таких как «Авито» и «Юла». В Пензенской области, как и в других регионах, распространены схемы, когда «покупатель» просит перейти по ссылке для оплаты товара, что ведет на фишинговую страницу, либо «продавец» требует предоплату за товар, который в действительности не существует.

Отдельную группу представляют инвестиционные мошенничества и лжеброкеры. Жителям области, особенно имеющим накопления, предлагают «гарантированный высокий доход» от вложений в криптовалюту, акции или «инновационные проекты». Как правило, первые выплаты действительно производятся, чтобы усыпить бдительность жертвы, после чего следует крупное хищение. По данным Центрального банка, именно эта категория мошенничества наносит наибольший материальный ущерб в расчете на одно преступление.

---

[1] В Пензенской области растет число киберпреступлений и мошенничеств. – URL: https://stolica58.ru/news/obcshestvo/v-penzenskoj (дата обращения: 02.05.2026).

[2] Информация о состоянии оперативной обстановки и результатов работы органов и подразделений внутренних дел Пензенской области за 2026 г. – URL: https://58.мвд.рф/document/61495918 (дата обращения: 07.05.2026).

Особого внимания заслуживает рост вымогательства в интернете: за январь–февраль 2026 г. число таких фактов увеличилось на 67% (с 6 до 10 случаев), что свидетельствует об освоении злоумышленниками новых методов давления, включая угрозы распространения компрометирующих данных. При этом снизилось количество традиционных компьютерных краж (–32%), неправомерного доступа к информации (–20%) и активности наркоторговцев с использованием ИТ (–13%).

Важным аспектом анализа является выявление групп пострадавших внутри региона. Данные, озвученные на брифинге в региональном правительстве с участием представителей УМВД, Министерства труда и Банка России, однозначно указывают на то, что наиболее часто жертвами кибермошенников становятся люди пожилого возраста.

Пензенская область характеризуется достаточно высокой долей граждан старшего поколения в структуре населения, что создает объективные предпосылки для повышенной уязвимости этой категории. Мошенники эксплуатируют доверчивость, недостаточную цифровую грамотность и эмоциональную отзывчивость пожилых людей. Особенно эффективными оказываются схемы «родственник в беде», «проблемы с банком» и «выигрыш приза». Именно для защиты этой группы населения губернатором Олегом Мельниченко был инициирован проект «Серебряная Пенза», в рамках которого юристы и психологи проводят занятия в небольших группах, обучая пенсионеров распознавать мошеннические звонки и правильно реагировать на них. В 2025 г. обучение прошли более 2,5 тысячи человек, а в 2026 г. проект расширен на все муниципальные образования области.[1]

Вместе с тем было бы ошибочно полагать, что жертвами кибермошенников становятся исключительно пенсионеры. Статистика свидетельствует о значительном числе пострадавших среди граждан трудоспособного возраста от 25 до 45 лет. Эта группа наиболее активно

[1] Разобраться в современных схемах обмана пожилым горожанам помогает губернаторский проект «Серебряная Пенза». – URL: https://pnzreg.ru/news/sotsialnaya-sfera/474410 (дата обращения: 02.05.2026).

пользуется интернет–банкингом, совершает покупки онлайн, инвестирует и берет кредиты. Именно на нее ориентированы схемы, связанные с «дополнительным заработком», «инвестиционными предложениями», а также мошенничества при продаже и покупке товаров на онлайн–площадках.

Люди среднего возраста часто переоценивают свою способность распознать обман и не следуют элементарным правилам кибергигиены, что делает их уязвимыми для более сложных и многоходовых комбинаций.

Еще одну группу риска составляют студенты и молодежь. Молодые люди нередко попадаются на уловки с «кэшбэком», «выигрышами в конкурсах», а также вовлекаются в преступные схемы в качестве так называемых дропперов – лиц, предоставляющих свои банковские карты для обналичивания похищенных средств. Как отметил Роман Сальников, случаи вовлечения молодежи в дропперство участились, и за это предусмотрена уголовная ответственность.[1]

Что касается географического распределения пострадавших внутри Пензенской области, то традиционно наибольшее количество киберпреступлений регистрируется в областном центре – городе Пензе, а также в закрытом административно–территориальном образовании Заречный и в Пензенском районе. Это объясняется как более высокой плотностью населения и уровнем цифровизации, так и большим количеством финансовых операций, совершаемых жителями этих территорий.

Переходя к показателям раскрываемости и ущербу от кибермошенничества, необходимо констатировать, что эта сфера остается одной из самых проблемных для правоохранительной системы.

Сложность раскрытия обусловлена рядом объективных факторов: анонимностью злоумышленников, использованием подменных номеров, VPN и анонимайзеров, выводом похищенных средств через дропперов и зарубежные счета, а также трансграничным характером многих преступлений,

[1] В Правительстве Пензенской области прошла пресс-конференция, посвященная профилактике мошеннических действий в сфере информационно-телекоммуникационных технологий. – URL: https://www.penza.kp.ru/daily/27766/5224560/?ysclid=mpbct9dfu68474985 (дата обращения: 02.05.2026).

когда колл–центры физически располагаются на территории других государств.

На заседании межведомственной группы 16 декабря 2025 г. отметили необходимость повышения качества работы на первоначальном этапе расследования, пока можно получить данные о транзакциях и цифровых следах.

Материальный ущерб от кибермошенничества в Пензенской области исчисляется сотнями миллионов рублей и продолжает оставаться значительным, несмотря на снижение числа преступлений.

По итогам 2025 г. общая сумма ущерба от зарегистрированных киберпреступлений превысила 1,1 миллиарда рублей. За первые два месяца 2026 г. ущерб составил более 130 миллионов рублей (по другим данным – свыше 133 миллионов). При этом особую тревогу вызывает низкий процент возмещения похищенных средств. В 2025 г. удалось вернуть потерпевшим около 20 миллионов рублей, что составляет менее двух процентов от общего ущерба. В 2026 г. за два месяца возвращено более 6 миллионов рублей – также крайне незначительная доля. По оконченным уголовным делам сумма причиненного ущерба за январь–февраль 2026 г. превысила 6,3 миллиона рублей, однако по приостановленным делам значится ущерб почти в 127 миллионов рублей, что наглядно демонстрирует, какой объем финансовых потерь граждан остается без перспективы возмещения.[1]

Прокуратура Пензенской области активно использует механизм гражданско–правовых исков для защиты прав потерпевших. В 2025 г. прокурорами предъявлено 158 исковых заявлений о взыскании в пользу потерпевших средств, похищенных неустановленными лицами, на общую сумму более 37 миллионов рублей. Из числа предъявленных исков рассмотрено и удовлетворено 104 на сумму свыше 18,5 миллиона рублей. Ранее, по данным за пять месяцев 2025 года, было подано 97 исков на 19

[1] Информация о состоянии оперативной обстановки в Пензенской области за январь – декабрь 2025 г. – URL: https://58.мвд.рф/document/61495918 (дата обращения: 07.05.2026).

миллионов рублей, удовлетворено 4 на 196 тысяч рублей. Рост удовлетворенных исков свидетельствует о постепенном повышении эффективности этой работы, однако по–прежнему значительная часть исков остается без удовлетворения либо находится на рассмотрении судов длительное время.

Положительным моментом является деятельность правоохранительных органов по изъятию и аресту имущества подозреваемых. В 2025–2026 г.г. конфисковано имущества на сумму свыше 4,3 миллиона рублей и наложен арест на ценности еще на 1,6 миллиона рублей. Добровольно пострадавшим возмещено около 1,6 миллиона рублей. Это хотя и не покрывает всех потерь, но демонстрирует, что работа в данном направлении ведется и приносит реальные результаты.

Следует отметить, что на снижение числа киберпреступлений в 2025 г. повлиял не только рост эффективности правоохранительной системы, но и некоторые нетрадиционные факторы. Как заявил министр региональной безопасности Пензенской области Василий Ложкин, ограничение мобильного интернета в регионе, введенное по ряду причин и вызвавшее общественное возмущение, неожиданно привело к снижению числа кибермошенничеств.

Сокращение возможностей онлайн–коммуникаций создало трудности для преступников, желающих влиять на потенциальных жертв через видеозвонки и онлайн–переписку.[1]

Важную роль в противодействии кибермошенничеству играют также законодательные изменения.

Как проинформировал председатель Законодательного собрания Пензенской области Вадим Супиков, в сентябре 2025 г. вступил в силу Федеральный закон № 41–ФЗ от 1 апреля 2025 г., который предоставил банкам право вводить ограничения на снятие наличных в банкоматах при подозрительных транзакциях. В таких случаях максимальная сумма снятия

[1] В Пензенской области отмечается снижение числа интернет-преступлений. – URL: https://pnzreg.ru/news/society/476303/ (дата обращения: 07.05.2026).

ограничивается 50 тысячами рублей в течение суток, а банк обязан незамедлительно уведомить владельца счета об установленном лимите посредством SMS, push–уведомления, электронного письма или телефонного звонка. Данные ограничения применяются выборочно и не затрагивают добросовестных пользователей.[1]

Кроме того, жителям Пензенской области рекомендовано использовать новую опцию назначения доверенных лиц для подтверждения денежных переводов и снятия наличных, что также повышает уровень финансовой защищенности. Прокуратура региона организовала «горячую линию» по вопросам противодействия хищениям с банковских карт и иным ИТ–преступлениям, что позволяет гражданам оперативно получать разъяснения и инициировать проверочные мероприятия.

По итогам анализа состояния и динамики кибермошенничества в Пензенской области можно сделать следующие выводы.

После значительного роста в 2023–2024 г. (+33,8%) с 2025 г. наблюдается устойчивое снижение числа киберпреступлений (–23,1% за год и –26% за первые два месяца 2026 г.), что опережает средние показатели по ПФО и России и свидетельствует об эффективности региональных мер.

Наиболее уязвимой группой остаются пожилые люди, для защиты которых успешно реализуется проект «Серебряная Пенза» (обучено более 2,5 тыс. человек в 2025 г.).

Несмотря на рост раскрываемости с 15% до 21%, этот показатель остаётся низким, а возврат средств потерпевшим не превышает 2% от общего ущерба (свыше 1,1 млрд рублей в 2025 г.), поскольку большинство дел приостанавливается за неустановлением виновных, а средства выводятся на зарубежные счета или в криптовалюту.

Снижение преступности достигнуто за счёт комплекса мер: совершенствования работы правоохранительных органов и банков,

[1] О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий: Федеральный закон от 01.04.2025 № 41-ФЗ (ред. от 31.07.2025) // Собрание законодательства РФ. – 2022. – № 14. – Ст. 1574.

законодательных ограничений, повышения цифровой грамотности населения и организационных ограничений мобильного интернета.

Дальнейшие усилия необходимо направить на повышение раскрываемости, межведомственное взаимодействие, продолжение просветительской работы среди всех групп населения и адаптацию к быстро меняющимся методам киберпреступников. Только комплексный подход позволит существенно снизить как количество мошенничеств, так и масштаб причиняемого ущерба.

3 Проблемы и основные направления совершенствования противодействия кибермошенничеству

В условиях стремительной цифровизации всех сфер жизни общества кибермошенничество превратилось в одну из наиболее масштабных и трудно раскрываемых угроз, что ставит перед правоохранительной системой комплексные правовые, технические и организационные проблемы, требующие безотлагательного решения.

На основе проведенного анализа мошенничества в цифровом пространстве можно выделить ключевые проблемы, две из которых носят правовой характер, а две другие – организационно–технологический и социальный. При этом важно подчеркнуть, что все указанные проблемы взаимосвязаны, и решение каждой из них требует комплексного подхода, при котором правовые изменения должны подкрепляться технологическими инновациями и наоборот.

Первая проблема, имеющая ярко выраженный правовой характер, заключается в несовершенстве уголовного и уголовно–процессуального законодательства Российской Федерации применительно к специфике кибермошенничества.

Как справедливо отмечает Клещина Е. Н., в Уголовном кодексе Российской Федерации установлена ответственность за компьютерные преступления, а также за ряд деяний, совершенных с использованием электронных средств платежа, в сфере компьютерной информации и посредством информационно–телекоммуникационных сетей, однако этого явно недостаточно.[1]

Во–первых, в законодательстве отсутствует легальное определение таких общественно опасных явлений, как кибербуллинг, кибертерроризм и киберэкстремизм, что затрудняет квалификацию соответствующих деяний и

[1] Клещина Е. Н. Проблемы и основные направления совершенствования правового регулирования противодействия киберпреступности // Государственная служба и кадры. – 2024. – № 4. – С. 240.

привлечение виновных к ответственности.

Во–вторых, название главы 28 УК РФ «Преступления в сфере компьютерной информации» устарело, поскольку подобные преступления могут совершаться не только с использованием компьютеров, но и с помощью любых электронных носителей, мобильных устройств и средств связи.

В–третьих, в УПК РФ до сих пор не закреплено понятие «электронные (цифровые) доказательства», что создает серьезные проблемы при собирании, проверке и оценке доказательств по уголовным делам о кибермошенничестве. Следователи и дознаватели вынуждены действовать в отсутствие единого порядка работы с электронными носителями информации, а также с информацией, извлеченной из мессенджеров, социальных сетей и иных интернет–ресурсов.

Кроме того, в УПК РФ отсутствуют такие следственные действия, как:

– осмотр сетевых информационных ресурсов без их физического изъятия;

– удаленное подключение к компьютерному оборудованию в процессе его работы;

– получение информации от операторов связи и провайдеров в режиме реального времени;

– прекращение электронно–почтовой корреспонденции и сообщений в мессенджерах.

Генеральный прокурор РФ И. Краснов также обращает внимание на то, что при расследовании преступлений, совершенных в виртуальном пространстве, обязательным условием является полная фиксация данных обо всех эпизодах противоправной деятельности и их последующий анализ, в том числе с использованием нейросетевых комплексов, что позволяет выявить уникальный цифровой след, характерный для каждого криминального деяния.[1]

[1] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации (утв. Генпрокуратурой России). – URL: https://www.consultant.ru/document/cons_doc_LAW_161817/ (дата обращения: 02.05.2026).

Однако отсутствие процессуального механизма фиксации и изъятия цифровых следов приводит к тому, что значительная часть кибермошенничеств остается нераскрытой. В качестве основных направлений совершенствования правового регулирования в данной сфере можно предложить следующие меры.

Необходимо внести изменения в УК РФ в части установления уголовной ответственности за новые виды преступлений, совершаемых с использованием электронных или информационно–телекоммуникационных технологий, включая кибермошенничество с использованием методов социальной инженерии, фишинга, вишинга и других технологий обмана. Целесообразно также переименовать главу 28 УК РФ, расширив ее предметное поле до «Преступлений в сфере цифровых и информационно–телекоммуникационных технологий».

Кроме того, требуется дополнить УПК РФ статьей, закрепляющей понятие и правовой режим электронных (цифровых) доказательств, с указанием их видов, требований к допустимости и порядка приобщения к уголовному делу. Важно также ввести в УПК РФ новые следственные действия, связанные с получением информации из информационных ресурсов, такие как «осмотр цифровой информации, содержащейся в информационно–телекоммуникационных сетях», «получение информации о соединениях между абонентами и (или) пользовательским оборудованием в режиме реального времени», а также «выемка электронной информации с удаленных серверов с применением средств криптографической защиты». Эти изменения позволят следователям более эффективно фиксировать цифровые следы кибермошенничества и использовать их в качестве полноценных судебных доказательств.[1]

Вторая проблема, также носящая правовой характер и тесно связанная с первой, заключается в отсутствии эффективного механизма международного

[1] Клещина Е. Н. Проблемы и основные направления совершенствования правового регулирования противодействия киберпреступности // Государственная служба и кадры. – 2024. – № 4. – С. 241.

сотрудничества в противодействии трансграничному кибермошенничеству и в разобщенности правовых норм различных государств. Киберпространство, как известно, не имеет государственных границ, и мошенники активно используют серверы, расположенные в юрисдикциях с мягким законодательством в сфере кибербезопасности, а также криптовалюты и другие анонимные платежные инструменты для вывода и легализации похищенных средств.

Как указывает Клещина Е. Н., Российская Федерация выступила инициатором разработки универсальной конвенции ООН о противодействии использованию информационно–коммуникационных технологий в преступных целях, и еще в 2017 г. МИД России представило в ООН соответствующий проект. Более того, 27 декабря 2019 г. по инициативе России была принята резолюция «Противодействие использованию информационно–коммуникационных технологий в преступных целях», а также принято решение о создании Специального комитета по разработке концепции ООН.[1]

Однако до настоящего времени универсальный международный договор так и не принят. Западные страны, как отметил министр иностранных дел С. Лавров, возражают против широкого охвата предлагаемой конвенции и предпочитают придерживаться более узкого документа – Конвенции Совета Европы о преступности в сфере компьютерной информации 2001 г. (Будапештской конвенции), к которой Россия долгое время не могла присоединиться по политическим причинам.

В результате правоохранительные органы Российской Федерации сталкиваются с серьезными трудностями при направлении международных запросов о правовой помощи, получении информации от зарубежных провайдеров и операторов связи, а также при розыске и экстрадиции лиц, совершивших кибермошенничество с использованием зарубежной инфраструктуры.

[1] Клещина Е. Н. Проблемы и основные направления совершенствования правового регулирования противодействия киберпреступности // Государственная служба и кадры. – 2024. – № 4. – С. 242.

Кроме того, различия в национальных законодательствах в части ответственности за киберпреступления, сроков давности, допустимости электронных доказательств и процедур их получения создают дополнительные барьеры.

Проблема усугубляется активным использованием мошенниками криптовалют, транзакции которых трудно отслеживать традиционными методами, а также технологий дипфейков и подмены номеров.

Основными направлениями совершенствования в данной сфере являются: продолжение активной дипломатической работы по принятию универсальной конвенции ООН о противодействии киберпреступности; развитие двусторонних и многосторонних соглашений о правовой помощи по делам о кибермошенничестве с государствами – участниками СНГ, Шанхайской организации сотрудничества, БРИКС и «Группы двадцати»; гармонизация национальных законодательств в части определения признаков киберпреступлений и стандартов работы с электронными доказательствами; создание международной системы оперативного обмена информацией о подозрительных криптовалютных транзакциях и о лицах, причастных к организации транснациональных мошеннических схем.

В рамках Содружества Независимых Государств уже приняты такие документы, как Модельный информационный кодекс 2008 г., Модельный закон «О важнейших объектах информационно–коммуникационной инфраструктуры» 2014 года, а в 2023 году – Рекомендации по вопросам профилактики и пресечения преступлений в сфере информационно–коммуникационных технологий. Однако эти акты носят рекомендательный характер, и требуется их имплементация в национальные законодательства всех государств–участников.

На уровне национального законодательства необходимо также разработать и принять отдельный федеральный закон, регулирующий порядок взаимодействия российских правоохранительных органов с иностранными провайдерами и операторами связи, включая механизмы получения

электронных доказательств, находящихся на серверах за пределами Российской Федерации, а также порядок признания и исполнения иностранных судебных поручений по делам о кибермошенничестве.

Третья проблема, не имеющая прямого правового характера, но тесно связанная с правоприменительной практикой, заключается в ведомственной разобщенности и недостаточной координации между правоохранительными органами, банковским сектором, операторами связи и иными участниками системы противодействия кибермошенничеству. Эффективное противодействие дистанционному мошенничеству требует скоординированного взаимодействия всех заинтересованных сторон, однако на практике наблюдается недостаточная интеграция и координация действий между ними. Каждое ведомство действует в рамках своей компетенции, зачастую дублируя функции друг друга либо, напротив, оставляя без внимания важные участки работы.

Например, правоохранительные органы инициируют процедуры блокировки банковских счетов, используемых в преступных схемах, однако скорость реагирования банков на такие запросы оставляет желать лучшего. Банки, в свою очередь, осуществляют мониторинг операций клиентов на предмет выявления подозрительных транзакций, но критерии подозрительности, установленные нормативными актами Банка России и Росфинмониторинга, не всегда позволяют своевременно распознать мошеннические схемы, особенно если они являются новыми и ранее не встречавшимися. Операторы связи и интернет–провайдеры обладают информацией о номерах телефонов, IP–адресах и других идентификаторах, используемых мошенниками, однако механизмы оперативной передачи этой информации в правоохранительные органы либо отсутствуют, либо являются недостаточно эффективными. Отсутствие единой межведомственной информационно–аналитической платформы, объединяющей данные всех указанных субъектов, приводит к тому, что информация о подозрительных операциях, мошеннических телефонных номерах и интернет–ресурсах

фрагментирована, а время между совершением преступления и блокировкой счетов или каналов связи оказывается достаточным для того, чтобы мошенники успели вывести и обналичить похищенные средства.

Как показывает практика, к моменту, когда потерпевший обращается в правоохранительные органы, а те направляют запрос в банк, деньги уже оказываются списанными и переведенными на счета «дропов» или «денежных мулов», а затем – в криптовалюту или за пределы юрисдикции Российской Федерации.

Основными направлениями совершенствования в этой части являются:

– создание единой межведомственной цифровой платформы для оперативного обмена информацией о кибермошенничестве, объединяющей правоохранительные органы, Банк России, коммерческие банки, операторов связи, интернет–провайдеров и Росфинмониторинг;

– разработка и утверждение четких регламентов межведомственного взаимодействия с указанием сроков реагирования и ответственности за их нарушение;

– внедрение автоматизированных систем мониторинга подозрительных финансовых операций и телефонных вызовов с использованием технологий искусственного интеллекта;

– создание специализированных подразделений в структуре МВД России, которые занимались бы исключительно противодействием кибермошенничеству и были бы оснащены современными программно–техническими средствами;

– усиление координации со стороны Генеральной прокуратуры Российской Федерации, которая могла бы осуществлять надзор за своевременностью и полнотой межведомственного взаимодействия.[1]

Необходимо законодательно обязать банки и операторов связи приостанавливать подозрительные операции и передавать информацию о них

[1] Калиев А. А. Киберпреступность в современном мире: основные понятия и тенденции: учебное пособие. – Косшы, 2023. – С. 67.

в уполномоченные органы в режиме реального времени. Также целесообразно внедрить на уровне всех операторов связи систему «антифрод» для блокировки вызовов с подменных номеров и создать единую базу данных о мошеннических номерах, банковских картах и интернет–ресурсах, доступную всем участникам системы противодействия.

Четвёртой проблемой противодействия кибермошенничеству является низкий уровень цифровой грамотности населения и технологическое отставание правоохранительных органов от методов, используемых преступниками. Граждане, особенно пожилого возраста, не обладают навыками распознавания фишинга, вишинга, дипфейков и вредоносного программного обеспечения. В то же время правоохранительные подразделения зачастую оснащены устаревшим оборудованием, а сотрудники не имеют достаточной квалификации в области цифровой криминалистики и блокчейн–аналитики. Это приводит к низкой раскрываемости и невозврату похищенных средств в большинстве случаев.

Основными направлениями совершенствования в данной сфере являются:

– реализация государственных программ повышения цифровой грамотности населения с охватом всех возрастных групп, особенно пожилых;

– создание государственных сервисов оперативного оповещения граждан о новых мошеннических схемах (через портал «Госуслуги», SMS–рассылки, банковские приложения);

– технологическое перевооружение правоохранительных органов: внедрение систем искусственного интеллекта для анализа больших данных, создание лабораторий цифровой криминалистики, обучение сотрудников блокчейн–аналитике и работе с дипфейками;

– приоритетное финансирование отечественных НИОКР в сфере кибербезопасности.

Проведённый анализ представленных проблем показывает, что их решение возможно только на основе комплексного подхода, включающего:

совершенствование законодательства об электронных доказательствах; активизацию взаимодействия в рамках ООН, СНГ, ШОС и БРИКС; создание единой межведомственной платформы для обмена информацией с банками и операторами связи; реализацию государственных программ цифровой грамотности и технологическое перевооружение с внедрением ИИ и блокчейн–аналитики.

Только такой комплексный подход позволит минимизировать экономические потери от кибермошенничества, укрепить доверие граждан к цифровой экономике и обеспечить экономическую безопасность Российской Федерации в условиях глобальной цифровизации.

ЗАКЛЮЧЕНИЕ

Проведённое исследование мошенничества в цифровом пространстве позволяет сформулировать ряд итоговых выводов, имеющих как теоретическое, так и прикладное значение.

В ходе работы установлено, что кибермошенничество представляет собой сложное, динамично развивающееся явление, органично вписавшееся в структуру современных общественных отношений, опосредованных информационно–телекоммуникационными технологиями. Российское законодательство, пройдя путь от полного отсутствия норм до разветвлённой системы, включающей ст. 159, 159.6, 272–274.2 УК РФ, в целом создало правовую основу для противодействия данным преступлениям.

Однако правоприменительная практика сталкивается с серьёзными трудностями, обусловленными как пробелами в нормативном регулировании (отсутствие легального определения электронных доказательств, устаревшее наименование главы 28 УК РФ), так и объективными свойствами цифровой среды – анонимностью, трансграничностью, высокой латентностью.

Ключевым выводом работы является необходимость различения общего мошенничества, совершённого с использованием цифровых технологий (социальная инженерия, фишинг, подмена номера), и специального состава, предусмотренного ст. 159.6 УК РФ, где хищение опосредовано прямым техническим вмешательством в компьютерную информацию. Предложенное авторское определение кибермошенничества охватывает обе группы деяний и может быть использовано в правотворческой и правоприменительной деятельности.

Криминологический анализ показал, что типичный киберпреступник – это мужчина 18–29 лет, нередко с техническим образованием, корыстной мотивацией, низкой эмпатией и иллюзией безнаказанности, причём почти половина действуют в организованных группах. Портрет жертвы, вопреки стереотипам, сместился в сторону экономически активного населения 25–44

лет (преимущественно женщины), хотя пожилые люди остаются наиболее уязвимой группой в силу демографических особенностей и успешности против них методов социальной инженерии.

Региональный анализ на примере Пензенской области выявил обнадёживающую тенденцию: после пикового роста в 2024 г. (+33,8%) с 2025 г. фиксируется устойчивое снижение числа киберпреступлений (–23,1% за год, –26% за первые два месяца 2026 г.), опережающее средние показатели по ПФО и России. Это снижение достигнуто за счёт комплекса мер: совершенствования работы правоохранительных органов и банков, законодательных ограничений (Федеральный закон № 41–ФЗ от 1 апреля 2025 г.), просветительского проекта «Серебряная Пенза» (обучено более 2,5 тыс. пенсионеров), а также, хотя и неоднозначных, организационных ограничений мобильного интернета. Вместе с тем раскрываемость остаётся низкой (около 21%), а возврат похищенных средств не превышает 2% от ущерба, превысившего в 2025 г. 1,1 млрд рублей. Большинство дел приостанавливается за неустановлением виновных, а средства выводятся на зарубежные счета или в криптовалюту.

Практическая значимость работы заключается в возможности использования сформулированных выводов и рекомендаций в трёх направлениях.

Во–первых, в правотворческой деятельности – для совершенствования уголовного и уголовно–процессуального законодательства (закрепление понятия электронных доказательств, введение новых следственных действий, переименование главы 28 УК РФ).

Во–вторых, в правоприменительной деятельности – для повышения качества расследования кибермошенничеств, правильной квалификации деяний и использования специальных экспертных знаний (информационно–технологической и информационно–технической экспертиз). В–третьих, в профилактической деятельности – для организации системного просвещения населения, особенно в рамках региональных проектов типа «Серебряная

Пенза», а также для создания единой межведомственной платформы обмена информацией между правоохранительными органами, банками и операторами связи.

Вместе с тем в ходе исследования выявились вопросы, остающиеся недостаточно изученными и требующие дальнейшей разработки.

Во–первых, это проблема международного сотрудничества: отсутствие универсальной конвенции ООН о противодействии киберпреступности и разобщённость правовых норм различных государств существенно затрудняют борьбу с трансграничным кибермошенничеством, особенно в части экстрадиции и получения электронных доказательств с зарубежных серверов.

Во–вторых, это технологический аспект: стремительное развитие дипфейков, генеративных нейросетей и квантовых технологий создаёт новые, ещё не изученные способы совершения мошенничества, к которым правоохранительная система может оказаться не готова. В–третьих, это криптовалютная проблематика: правовой статус криптовалют как предмета преступления, методика отслеживания блокчейн–транзакций и механизмы возврата похищенных цифровых активов остаются слабо разработанными как в теории, так и на практике.

Перспективы дальнейших исследований в данной сфере лежат в нескольких направлениях.

Во–первых, необходимо проведение сравнительно–правовых исследований с зарубежными странами, имеющими более развитую практику противодействия кибермошенничеству (США, Великобритания, Германия), с целью адаптации их положительного опыта к российским реалиям.

Во–вторых, требуется разработка криминалистических методик расследования новых видов кибермошенничества, связанных с использованием искусственного интеллекта, технологии интернета и криптовалют.

В–третьих, важно продолжение региональных криминологических

исследований, поскольку анализ на примере Пензенской области показал, что эффективные профилактические меры могут иметь ярко выраженную региональную специфику, что требует дальнейшего изучения и распространения лучших практик.

Таким образом, противодействие кибермошенничеству не может ограничиваться только уголовно–правовыми мерами. Оно требует комплексного, междисциплинарного подхода, объединяющего усилия законодателя, правоприменителя, банковского сектора, операторов связи, IT–специалистов и широких слоёв населения.

Только сочетание правовых, организационных, технических и образовательных мер позволит существенно снизить уровень киберпреступности, минимизировать имущественный ущерб граждан и обеспечить экономическую безопасность государства в условиях глобальной цифровизации.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

Нормативно–правовые акты

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках в Конституции РФ от 30.12.2008 № 6–ФКЗ, от 30.12.2008 № 7–ФКЗ, от 05.02.2014 № 2–ФКЗ, от 21.07.2014 № 11–ФКЗ, от 14.03.2020 № 1–ФКЗ, от 4.10.2022 № 5– ФКЗ, от 4.10.2022 № 6–ФКЗ, от 4.10.2022 № 7–ФКЗ, от 4.10.2022 № 8–ФКЗ) // Собрание законодательства РФ. – 1996. – № 31. – Ст. 4398.

2. Уголовный кодекс Российской Федерации от 13.06.1996 № 63–ФЗ (ред. от 09.04.2026) // Собрание законодательства РФ. – 1996. – № 43. – Ст. 4190.

3. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51–ФЗ (ред. от 08.08.2024) // Собрание законодательства РФ. – 1994. –№32. – Ст. 3301.

4. О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий: Федеральный закон от 01.04.2025 № 41–ФЗ (ред. от 31.07.2025) // Собрание законодательства РФ. – 2022. – № 14. – Ст. 1574.

5. О внесении изменений в Уголовный кодекс Российской Федерации: Федеральный закон от 30.11.2024 № 421–ФЗ (ред. от 11.12.2024) // Собрание законодательства РФ. – 2022. – № 29 (ч.IV). – Ст. 7412.

6. О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно–процессуальный кодекс Российской Федерации: Федеральный закон от 14.07.2022 № 260–ФЗ (ред. от 14.07.2022) // Собрание законодательства РФ. – 2022. – № 29 (ч.II). – Ст. 5227.

7. О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации: Федеральный закон от 29.11.2012 №207–ФЗ (ред. от 3.07.2016) // Собрание

законодательства РФ. – 2012. – № 49. – Ст. 6752.

8. О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации: Федеральный закон от 07.12.2011 № 420–ФЗ (ред. от 03.07.2016) // Собрание законодательства РФ. – 2011. – № 50. – Ст. 7362.

9. О государственной тайне: Закон РФ от 21.07.1993 № 5485–I (ред. от 08.08.2024) // Собрание законодательства РФ. – 1997. – № 41. – Ст. 4673.

10. Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента РФ от 05.12.2016 № 646 (последняя редакция) // Собрание законодательства РФ. – 2016. – № 50. – Ст. 7074.

11. Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации (утв. Генпрокуратурой России). – URL: https://www.consultant.ru/document/cons_doc_LAW_161817/ (дата обращения: 02.05.2026).

12. Методические рекомендации по вопросам профилактики преступлений, совершаемых с использованием информационно–коммуникационных технологий, и мерам противодействия им. – URL: https://www.garant.ru/products/ipo/prime/doc/412408244/(дата обращения: 07.05.2026).

13. По делу о проверке конституционности части второй статьи 128.1 Уголовного кодекса Российской Федерации в связи с жалобой гражданки Роговой Лилии Геннадьевны: Постановление Конституционного Суда РФ от 04.12.2025 № 43–П. – URL**:** https://www.consultant.ru/document/cons_doc_LAW_520623/(дата обращения: 07.05.2026).

14. О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно–телекоммуникационных сетей, включая сеть «Интернет»:

Постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 (ред. от 15.12.2022) // Бюллетень Верховного Суда РФ. – 2023. – № 3.

15. О судебной практике по делам о мошенничестве, присвоении и растрате: Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 (ред. от 15.12.2022) //Российская газета. – 2017. – № 280.

16. О модельном законе «О критически важных объектах информационно–коммуникационной инфраструктуры»: принят в г. Санкт–Петербурге 28.11.2014 (Постановление № 41–22) / Межпарламентская Ассамблея государств–участников СНГ. – URL: https://base.garant.ru/71871816/ (дата обращения: 07.05.2026).

Учебная и научная литература

17. Зуев С. В. Расследование преступлений в сфере компьютерной информации и электронных средств платежа: учебник для вузов / С. В. Зуев, В. Б. Вехов. – М.: Юрайт, 2026. – 243 с.

18. Калиев А. А. Киберпреступность в современном мире: основные понятия и тенденции: учебное пособие / А. А. Калиев. – Косшы, 2023. – 103 с.

19. Петраков С. В. Раскрытие и расследование преступлений, совершаемых с использованием информационно–телекоммуникационных технологий или в сфере компьютерной информации: учебное пособие / С. В. Петраков, А. Ю. Ушаков, А. А. Попов, К. Н. Дудаль. – СПб.: Санкт–Петербургская академия Следственного комитета РФ, 2021. – 84 с.

20. Поляков В. В. Основы методики расследования компьютерных преступлений: учебное пособие / В. В. Поляков. – Барнаул: Алтайский университет, 2024. – 121 с.

21. Попов А. Н. Преступления в сфере компьютерной информации: учебное пособие / А. Н. Попов. – СПб.: Санкт–Петербургский юридический институт (филиал) Университета прокуратуры РФ, 2018. – 68 с.

22. Раменская, В. С. Уголовное право. Уголовный процесс. Криминология: учебное пособие / В. С. Раменская, Е. И. Думанская, Н. А.

Жумаканова; под общ. ред. Е. Г. Шабловой. – Екатеринбург Уральский университет, 2023. – 248 с.

23. Савельев Д. В. Уголовное право. Общая часть: учебник для вузов / Д. В. Савельев. – М.: Юрайт, 2025. – 374 с.

24. Уторова Т. Н. Преступления в сфере информационной безопасности: учебное пособие / Т. Н. Уторова, Л. А. Колпакова. – Вологда: Северо–Западный ин–т (филиал) Ун–та им. О. Е. Кутафина (МГЮА), 2024. – 193 с.

Публикации в научных журналах, сборниках и СМИ

25. Айнутдинова К. А. Виктимологические особенности киберпреступности в условиях цифровой трансформации общества: материалы национальной научно–практической конференции в 2–х частях / К. А. Айнутдинова. – Казань: ТИСБИ, 2022. – С.34–40.

26. Бабурин В. В. Криминологическая характеристика личности киберпреступника в Российской Федерации и Республике Казахстан / В. В. Бабурин, К. О. Карабеков // Психопедагогика в правоохранительных органах. – 2024. – № 1 (96). – С. 113–119.

27. Белевитина Ю. В. Криминологический портрет личности киберпреступника в современной России / Ю. В. Белевитина // Инновационная наука. – 2022. – № 12–2. – С. 61–64.

28. Витвицкая С. С. Киберпреступления: понятие, классификация, международное противодействие / С. С. Витвицкая, А. А. Витвицкий, Ю. И. Исакова // Правовой порядок и правовые ценности. – 2023. –№ 1. – С. 126–136.

29. Гюльалиева Р. А. Зарубежный опыт борьбы с киберпреступлениями / Р. А. Гюльалиева, А. Р. Алиев // Мир науки и мысли. – 2023. – № 1. – С. 56 – 59.

30. Дрёмин А. А. Современное состояние и динамика преступности мошенничества с использованием электронных средств платежа в 2025 году / А. А. Дрёмин, С. А. Дробот // Вестник науки. – 2025. – № 6. – С. 72 – 84.

31. Жижина М. В. Содержательная составляющая преступлений в

сфере компьютерной информации в Российской Федерации и за рубежом / М. В. Жижина, Д. В. Завьялова // Российский следователь. – 2025. – № 8. – С. 6 – 9.

32. Китайкина О. О. Российское законодательство об уголовной ответственности за преступления в сфере компьютерной информации: история и современность / О. О. Китайкина // Научный формат. – 2020. – №12(15). – С.20 – 25.

33. Клещина Е. Н. Проблемы и основные направления совершенствования правового регулирования противодействия киберпреступности / Е. Н. Клещина // Государственная служба и кадры. – 2024. – № 4. – С. 240 – 245.

34. Клишков В. Б. Киберпреступность: понятие, признаки, основные направления противодействия / В. Б. Клишков, Е. В. Стебенева, М. А. Яковлева // Вестник Нижегородского университета им. Н.И. Лобачевского. – 2022. – № 4. – С. 106 –114.

35. Кузнецова А. П. Позиция Пленума о квалификации мошенничества требует уточнения / А. П. Кузнецова // Российская юстиция. – 2015. –№5. – С.69–75.

36. Кучерков И. А. О понятии «киберпреступление» в законодательстве и научной доктрине / И. А. Кучерков // Информационное право. – 2019. – №10. – С.78–81.

37. Муллаярова П. А. Психологический портрет киберпреступника / П. А. Муллаярова // Международный журнал гуманитарных и естественных наук. – 2021. – №56. – С.116 –118.

38. Номоконов В. А. Киберпреступность как новая криминальная угроза / В. А. Номоконов, Т. Л. Тропина // Криминология интернет–пространства. – 2012. – №12.– С.45 –55.

39. Харина Е. А. К вопросу об эффективности расследования мошенничества в сфере компьютерной информации / Е. А. Харина // Российский следователь. – 2024. – № 12.– С.15 – 19.

40. Чимаров С. Ю. Зарубежный опыт противодействия киберпреступности: в контексте опоры полиции на потенциал общественности / С. Ю. Чимаров, В. С. Бялт // Международный журнал гуманитарных и естественных наук. – 2023. – № 1–3 (76). – С.23–28.

41. Шевко Н. Р. Меры противодействия киберпреступности: зарубежный опыт / Н. Р. Шевко, С. Я. Казанцев, Э. Н. Хисамутдинова // Криминологический журнал. – 2023. – № 1. – С.144–147.

42. Яким А. Д. ChatGPT и информационные технологии в аспекте киберпреступности / А. Д. Яким // Проблемы противодействия киберпреступности: Материалы международной научно-практической конференции, Москва, 28 апреля 2023 года. – М.: Московская академия Следственного комитета РФ, 2023. – С. 240-244.

43. Ян А. С. Киберпреступность: особенности, развитие и мотивы киберпреступности / А. С. Ян // Вестник науки. – 2025. – № 10 (91). – С.434–438.

Источники на электронных носителях

44. В Пензенской области отмечается снижение числа интернет–преступлений. – URL: https://pnzreg.ru/news/society/476303/ (дата обращения: 07.05.2026).

45. В Пензенской области растет число киберпреступлений и мошенничеств. – URL: https://stolica58.ru/news/obcshestvo/v–penzenskoj (дата обращения: 02.05.2026).

46. В Правительстве Пензенской области прошла пресс–конференция, посвященная профилактике мошеннических действий в сфере информационно–телекоммуникационных технологий. – URL: https://www.penza.kp.ru/daily/27766/5224560/?ysclid=mpbct9dfu68474985 (дата обращения: 02.05.2026).

47. Информация о состоянии оперативной обстановки в Пензенской области за январь–декабрь 2024 г. – URL: https://stolica58.ru/news/obcshestvo/v–penzenskoj (дата обращения: 02.05.2026).

48. Информация о состоянии оперативной обстановки в Пензенской области за январь – декабрь 2025 г. – URL: https://58.мвд.рф/document/61495918 (дата обращения: 07.05.2026).

49. Информация о состоянии оперативной обстановки и результатов работы органов и подразделений внутренних дел Пензенской области за 2026 г. – URL: https://58.мвд.рф/document/61495918 (дата обращения: 07.05.2026).

50. НТВ и научный сотрудник Лаборатории финансовой грамотности ЭФ Марат Сафиулин о финансовой пирамиде QBF. – URL: https://www.econ.msu.ru/about/comments/Article.20250421114702_9176/ (дата обращения: 02.05.2026).

51. Основные сведения о работе прокуратуры Пензенской области за 12 месяцев 2025 года. – URL: https://epp.genproc.gov.ru/ru/proc_58/activity/statistics/office/result/e8389158/ (дата обращения: 07.05.2026).

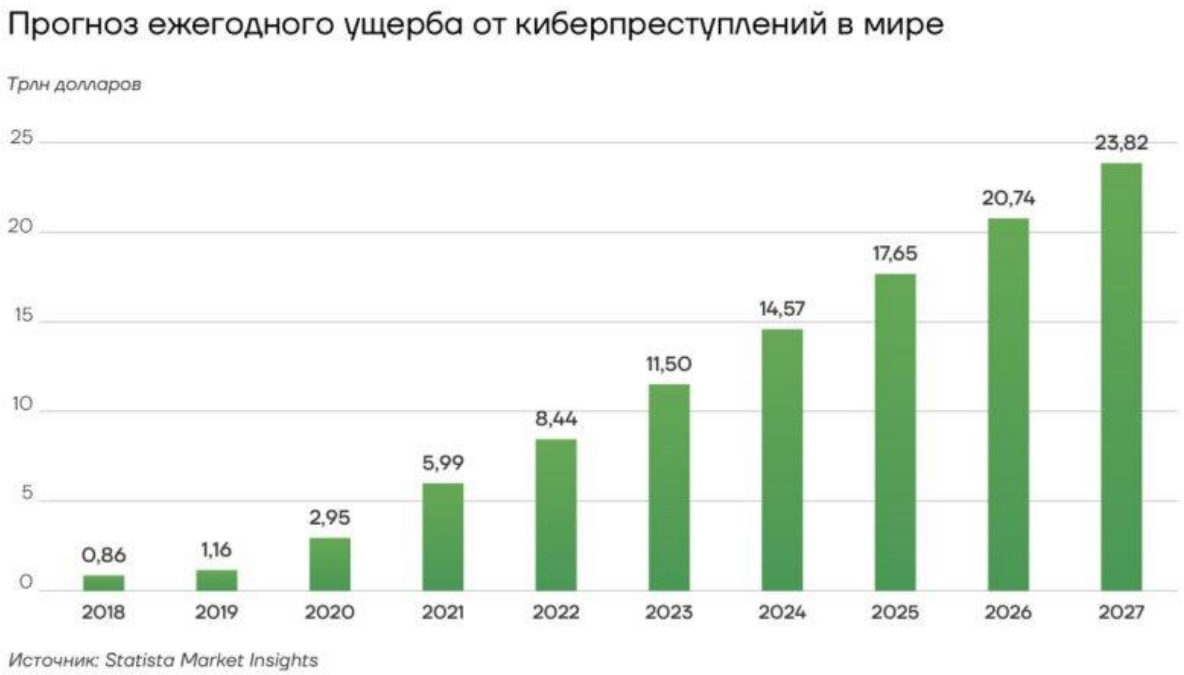
52. Разобраться в современных схемах обмана пожилым горожанам помогает губернаторский проект «Серебряная Пенза». – URL: https://pnzreg.ru/news/sotsialnaya–sfera/474410 (дата обращения: 02.05.2026).

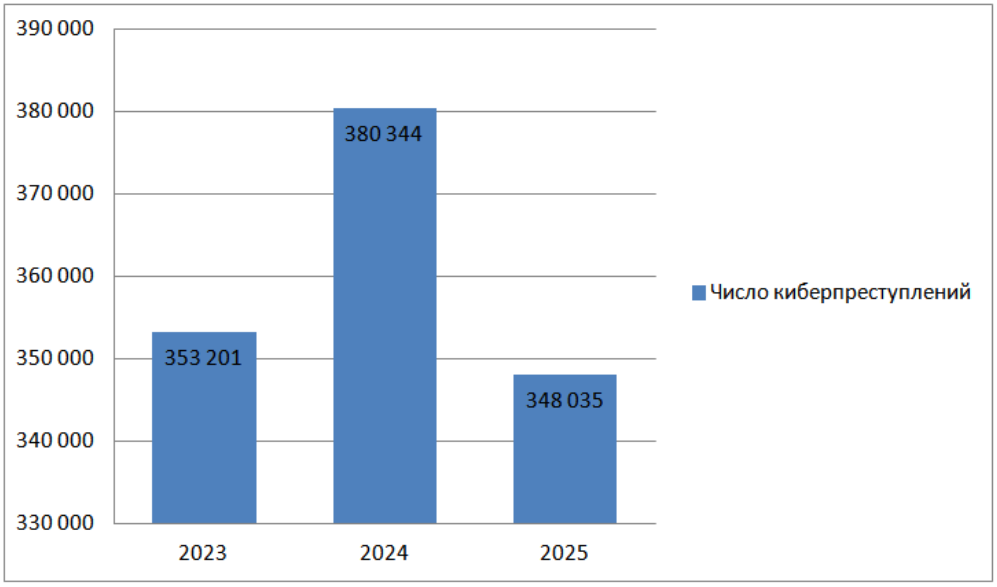
53. Состояние преступности в России за январь – декабрь 2025 г. – URL: https://мвд.рф/reports/item/77848182// (дата обращения: 02.05.2026).

54. Ущерб от киберпреступлений вырастет на треть за следующие 4 года: институт изучения мировых рынков. – URL: https://worldmarketstudies.ru/article/userb–ot–kiberprestuplenij–vyrastet–na–tret–za–sleduusie–4–goda/ (дата обращения: 02.05.2026).

Приложение А

ГЛОБАЛЬНЫЙ ПРОГНОЗ УЩЕРБА ОТ КИБЕРПРЕСТУПЛЕНИЙ ПО ГОДАМ В МИРЕ



Приложение Б

ДИНАМИКА ЧИСЛА ЗАРЕГИСТРИРОВАННЫХ МОШЕННИЧЕСТВ (СТ. 159–159.6 УК РФ) В РОССИЙСКОЙ ФЕДЕРАЦИИ ЗА 2023–2025 ГГ.