УГОЛОВНО-ПРАВОВЫЕ НАУКИ / CRIMINAL-LEGAL SCIENCES

Редактор рубрики *П. А. Кабанов* / Rubric editor *P. A. Kabanov*

Научная статья

BY-NC 4.0

УДК / UDC 343.9:[343.3/.7:004](470+571) **https://doi.org/10.21202/2782-2923.2026.1.190-206**

А. К. Жарова[1],
Е. С. Анисимов[1]

[1] *Финансовый университет при Правительстве Российской Федерации, г. Москва, Россия*

Анализ динамики киберпреступности в России

Контактное лицо:
Жарова Анна Константиновна, доктор юридических наук, доцент, профессор, Финансовый университет при Правительстве Российской Федерации
E-mail: anna_jarova@mail.ru
ORCID: http://orcid.org/0000-0002-2981-3369
Web of Science Researcher ID: H-4012-2015
eLIBRARY SPIN-код: 2240-1467

Анисимов Ефим Сергеевич, аспирант, Финансовый университет при Правительстве Российской Федерации
E-mail: EAnisimov_Sci@mail.ru
ORCID: http://orcid.org/0000-0002-2632-4439
eLIBRARY SPIN-код: 4954-5623

Аннотация

Цель: выявление основных тенденций, закономерностей и факторов, влияющих на количество зарегистрированных киберпреступлений и уровень их раскрываемости на основе анализа сведений о состоянии преступности в Российской Федерации за период с января 2022 г. по сентябрь 2025 г.

Методы: в статье используются всеобщий диалектический метод познания, а также общенаучные (анализ, синтез, индукция, дедукция) и частнонаучные методы исследования (формально-юридический).

Результаты: анализ статистических данных о зарегистрированных киберпреступлениях за 2022–2025 гг. позволил выявить следующие закономерности. В первый квартал 2025 г. и на протяжении полных 2023 и 2024 гг. наблюдалось устойчивое повышение количества киберпреступлений в сравнении с численными показателями за тот же период предыдущих лет. При этом показатели раскрываемости преступлений являются ежегодно высокими в январе каждого года. Объяснить это можно сочетанием организационных, процессуальных и сезонных факторов: активизацией работы правоохранительных органов; особенностями статистического учета и перераспределением ресурсов в условиях снижения других видов преступности. Позитивными наблюдениями стали незначительное замедление роста количества киберпреступлений во втором квартале 2025 г. (показатели на уровне II квартала 2024 г.), а также значительное их снижение в третьем квартале 2025 (–15 % в июле 2025 г. и почти –24 % в августе – сентябре по сравнению с июнем 2025 г.). Говорить о переломе тенденции роста количества киберпреступлений на основании

© Жарова А. К., Анисимов Е. С., 2026

шести месяцев преждевременно. Однако этого достаточно, чтобы сделать вывод о наличии сигнала в пользу скорого перелома в тенденции роста количества киберпреступлений. В работе отмечается, что период снижения совпал со вступлением в силу изменений в федеральном законодательстве, закрепивших основы создания и функционирования Государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий.
Научная новизна: представлен детальный анализ динамики количества зарегистрированных киберпреступлений и показателей их раскрываемости. Обозначены факторы сезонности в динамике регистрируемой киберпреступности. Отмечено совпадение запуска межведомственной платформы противодействия киберпреступлениям со снижением количества зарегистрированных киберпреступлений.
Практическая значимость: результаты исследования могут использоваться при совершенствовании уголовного и уголовно-процессуального законодательства; для нормативного регулирования в области оперативно-разыскной деятельности; повышения эффективности работы правоохранительных органов, а также в целях прогнозирования состояния киберпреступности.

Ключевые слова:
уголовно-правовые науки, криминология, преступность, киберпреступность, компьютерные преступления, раскрываемость, наказание

Как цитировать статью: Жарова, А. К., Анисимов, Е. С. (2026). Анализ динамики киберпреступности в России. *Russian Journal of Economics and Law*, *20*(1), 190–206. https://doi.org/10.21202/2782-2923.2026.1.190-206

Scientific article

A. K. Zharova[1],
E. S. Anisimov[1]

[1] *Financial University under the Government of the Russian Federation, Moscow, Russia*

Analysis of the cybercrime dynamics in Russia

Contact:
Anna K. Zharova, Dr. Sci. (Law), Associate Professor, Professor, Financial University under the Government of the Russian Federation
E-mail: anna_jarova@mail.ru
ORCID: http://orcid.org/0000-0002-2981-3369
Web of Science Researcher ID: H-4012-2015
eLIBRARY SPIN-code: 2240-1467

Efim S. Anisimov, postgraduate student, Financial University under the Government of the Russian Federation
E-mail: EAnisimov_Sci@mail.ru
ORCID: http://orcid.org/0000-0002-2632-4439
eLIBRARY SPIN-code: 4954-5623

Abstract
Objective: to identify the main trends, patterns and factors affecting the number of registered cybercrimes and their detection rate by analyzing the state of crime in the Russian Federation from January 2022 to September 2025.
Methods: the article uses the universal dialectical method of cognition, as well as general (analysis, synthesis, induction, deduction) and specific (formal-legal) scientific research methods.
Results: analysis of statistical data on registered cybercrimes for 2022–2025 revealed the following patterns. In the first quarter of 2025 and throughout the full years 2023 and 2024, there was a steady increase in the number of cybercrimes compared to the same period of previous years. At the same time, crime detection rates are annually high in January of each year. This is due to a combination of organizational, procedural, and seasonal factors: intensive law enforcement activities; peculiarities of statistical accounting and redistribution of resources under a decrease in other types of crime. Positive observations were

a slight slowdown in the growth rate of cybercrimes in the second quarter of 2025 (indicators at the level of the second quarter of 2024) and a significant decrease in the third quarter of 2025 (–15 % in July 2025 and almost –24 % in August–September compared to June 2025). Based on six months, one cannot talk about breaking a trend of increased number of cybercrimes. However, this allows concluding that there is a signal in favor of such a break. The authors note that the reduction coincided with the changes in federal legislation. They stipulated the bases for the creation and functioning of the State Information System for countering offenses committed using information and communication technologies.
Scientific novelty: the article presents a detailed analysis of the dynamics of registered cybercrimes and their detection, indicating the seasonality factors. The launch of an interagency cybercrime counteraction platform coincided with a decrease in the number of registered cybercrimes.
Practical significance: the results can be used to improve criminal and criminal-procedural legislation, regulation in the field of operational investigative activities, to increase the effectiveness of law enforcement agencies, and to predict the state of cybercrime.

Keywords:
criminal-legal sciences, criminology, crime, cybercrime, computer crimes, detection, punishment

For citation: Zharova, A. K., & Anisimov, E. S. (2026). Analysis of the cybercrime dynamics in Russia. *Russian Journal of Economics and Law*, *20*(1), 190–206. (In Russ.). https://doi.org/10.21202/2782-2923.2026.1.190-206

Введение

Преступность в сфере компьютерной информации или с использованием информационно-телекоммуникационных технологий – это глубоко социальное явление, затрагивающее экономику, культуру, психологию и структуру общества. Анализ факторов риска, последствий и стратегий противодействия требует комплексного междисциплинарного подхода.

Применение информационных технологий (далее – ИТ) позволяет преступникам масштабировать преступления, совершаемые с использованием информационно-телекоммуникационных технологий, и способствует формированию международной преступности в информационной сфере (Баранов, Соломатина, 2023; Azhibayev & Dzhanadilov, 2018). Этот тезис подтверждается ежегодным увеличением числа таких преступлений. Но функционал ИТ также позволяет и уйти от ответственности, тем самым процесс сопровождается ростом числа нераскрытых преступлений.

Преступность в информационной сфере отличается от других видов преступности своими ключевыми элементами: квалификацией преступников, применением ИТ для реализации преступного умысла и спецификой общественных отношений, на которые посягают преступники (Sarkar & Shukla, 2023). В соответствии с отчетными материалами состоявшегося координационного совещания по вопросам компьютерных преступлений под председательством Генерального прокурора Российской Федерации, «в октябре 2024 г. уровень раскрываемости преступлений в сфере ИТ снизился до 25,9 %... Эта тенденция наблюдается на фоне стабильно высокого количества совершаемых преступлений в сфере ИТ, несмотря на внедрение дополнительных механизмов противодействия»[1]. Рост количества преступлений, совершаемых с использованием ИТ, также подтверждает МВД России и фиксирует, что «доля таких преступлений составила 40 % от общего числа правонарушений в 2024 г.»[2]. «Суммарные потери от киберпреступлений сейчас – более $ 1 трлн в год, в том числе 600 млрд руб. в России»[3].

[1] Под председательством Игоря Краснова состоялось координационное совещание по вопросам противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных сетей, цифровой валюты и компьютерной информации. (2024, 10 октября). Генеральная прокуратура Российской Федерации. https://epp.genproc.gov.ru/web/gprf/mass-media/news?item=98418092

[2] Число киберпреступлений в России. TAdviser. https://www.tadviser.ru/index.php/Статья:Число_киберпреступлений_в_России

[3] Дорожная карта развития «сквозной» цифровой технологии «Квантовые технологии» (Документ опубликован не был). СПС «КонсультантПлюс».

Таким образом, на фоне увеличивающегося количества преступлений, совершаемых с использованием ИТ, снижается уровень их раскрываемости. Эта ситуация ярко демонстрирует важность темы, исследуемой в статье. Чтобы лучше понять текущую ситуацию, авторы проанализировали статистические данные о динамике преступлений, которые в соответствии с «Перечнем № 25 преступлений, совершенных с использованием (применением) информационно-телекоммуникационных технологий или в сфере компьютерной информации» (далее – Перечень № 25), размещенным в Указании Генпрокуратуры России № 462/11, МВД России № 2 от 25.06.2024[4], отнесены к этому виду преступлений без дополнительных условий.

Авторы статьи исследовали причины колебаний показателей, представили выявленные зависимости и обосновали результаты. Для этого были проанализированы официальные статистические данные, подготавливаемые Главным информационно-аналитическим центром МВД России (ГИАЦ МВД России), а также материалы из аналитических отчетов российских аналитических агентств: Агентства правовой информации и TAdviser.

Результаты исследования

1. Подходы к определению ИТ-преступлений

Термин «ИТ-преступления» интуитивно понятен многим. Его первыми начали использовать в учебных работах (Курушин, Минаев, 1998). Но в настоящее время широкий спектр функциональных возможностей ИТ демонстрирует узость термина «компьютерные преступления» для охвата всех преступлений, совершаемых с использованием ИТ (Жарова, 2023a; Onwuadiamu, 2025). Глава 28 УК РФ «Преступления в сфере компьютерной информации» также не включает все возможные преступления, совершаемые с использованием ИТ, например, различные виды компьютерных атак, фишинг, иные мошеннические действия в информационном пространстве и др. (Dremliuga et al., 2020; Жарова, 2023b).

Сегодня в научной литературе и правовых актах представлен широкий спектр терминов в данной области, например: *IT*-преступления[5, 6] (Al Makhmari et al., 2024; Al Nagrash et al., 2024; Alnakeep, 2022; Younies & Al-Tawil, 2020); преступления в сфере ИТ[7, 8] (Shukan et al., 2019); киберпреступления[9] (Агравал, 2023); преступления, совершенные с использованием (применением) информационно-телекоммуникационных технологий или в сфере компьютерной информации[10] (Елин, 2022).

Разнообразие терминов объясняется тем, что ИТ и их функциональные возможности привели к появлению новых схем совершения противоправных действий, видов преступлений, для обозначения которых требуются новые термины. Причем каждый из вышеперечисленных терминов отражает подход, принятый в конкретной научной области. Например, термин «ИТ-преступления» фокусируется на использовании ИТ для совершения преступления (Елин, Жарова, 2009; Унукович, 2021). Преступления в сфере компьютерной информации акцентируют внимание на предмете преступления – информации, содержащейся в компьютерных системах (Быкова, Казаков, 2024). Термин «киберпреступления» часто используется для обозначения всех видов преступлений, совершаемых в информационной сфере, независимо от того, какие технологии были использованы в преступных целях для нарушения общественных отношений.

Под компьютерным преступлением Е. А. Русскевич предлагает понимать противоправные действия, в которых способ их совершения обусловлен цифровой природой объекта преступления (Русскевич, 2025). В работе Е. А. Россинской в группу компьютерных объединяются все преступления с применением компьютерных

---

[4] Указание Генпрокуратуры России № 462/11, МВД России № 2 от 25.06.2024 «О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности». СПС «КонсультантПлюс».

[5] В России в 2024 году IT-преступления достигли пика за последние пять лет. (2025, 27 января). Информационное агентство ТАСС. https://tass.ru/proisshestviya/22978955

[6] Приказ МВД России № 878 от 25.11.2019. (2019). СПС «КонсультантПлюс».

[7] Указ Президента РФ от 16.05.2022 № 288. СЗ РФ 2022, 21, ст. 3426.

[8] О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации. № 41-ФЗ от 01.04.2025. (2025). СЗ РФ, № 14, ст. 1574.

[9] Распоряжение Правительства РФ № 830-р от 07.04.2025. (2025). СЗ РФ, 16, ст. 2060.

[10] Приказ Генпрокуратуры России № 746 от 09.12.2022. (2023). Законность, 2.

технологий, независимо от их состава (Россинская, 2021). К. Н. Евдокимов отмечает сложность в квалификации преступлений в сфере компьютерной информации и возможность отнесения к ним преступных деяний, в которых информация и информационные технологии являются средством их совершения (Евдокимов, 2025).

В работе Д. В. Жмурова преступления, совершенные с использованием информационно-телекоммуникационных технологий, и преступления в сфере компьютерной информации составляют киберпреступность (Жмуров, 2024). В свою очередь важно понимать значение приставки «кибер-». Как указывается в работе Ю. К. Язова, киберпространство – часть информационного пространства, в котором циркулирует цифровая информация и функционируют цифровые устройства ее обработки (Язов, 2025). Таким образом, представленная в документационной или аналоговой форме информация не входит в киберпространство, и, следовательно, связанные с такой информацией преступления не относятся к киберпреступности. Возвращаясь к рассматриваемым в настоящей работе группам преступлений, следует упомянуть, что в Перечне № 25 также перечислены способы совершения преступления, отметка которых является определенным условием отнесения к Перечню № 25 ряда преступлений. Среди прочего к способам совершения преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, относятся следующие:

– с применением расчетных (пластиковых) карт, отметка о чем проставляется при непосредственном использовании карт при совершении преступления;

– использование специальных средств и техники для компрометации банковских устройств самообслуживания (банкоматов, терминалов).

Если остальные входящие в Перечень неупомянутые 23 способа совершения преступлений явно связаны с цифровой информацией или цифровыми устройствами ее обработки, то обозначенные два способа требуют отдельного уточнения. Расчетные карты относятся к электронным средствам платежа, которые, согласно Федеральному закону «О национальной платежной системе», являются средством или способом, позволяющим проводить определенные операции в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации и других технических устройств[11]. Таким образом, расчетные карты являются частью системы безналичных расчетов, основанных на ИТ; все связанные с расчетными картами операции представлены именно в цифровой форме. Носитель информации в рамках большинства используемых сегодня в России расчетных карт – также цифровой, а именно микропроцессор. Следовательно, преступления с использованием расчетных карт относятся к киберпространству.

Относительно применения специальных средств для компрометации банкоматов и терминалов стоит обратить внимание, что банковские устройства самообслуживания – цифровые, поэтому они являются объектами киберпространства, выступающими в данном случае в качестве предмета преступления (Елин, Жарова, 2009). В связи с чем преступления, выражающиеся в компрометации таких устройств, допустимо относить к киберпреступлениям: цифровая природа объекта информатизации как предмета преступного посягательства обуславливает связь таких преступлений с киберпространством.

По причине такого терминологического разнообразия, а также в силу установленного отношения к киберпространству рассматриваемых групп преступлений, в статье мы будем использовать обобщающий термин – «киберпреступления». Дополнительным основанием использования термина «киберпреступления» является его применение в правовых актах, например, «подразделение по борьбе с киберпреступлениями»[12].

Разнообразие киберпреступлений отражает отмеченный ранее Перечень № 25, в котором выделяются: преступления, относящиеся к перечню без дополнительных условий, и преступления, относящиеся к перечню при наличии определенных условий.

К киберпреступлениям без дополнительных условий отнесены: п. «г» ч. 3 ст. 158 УК РФ; ст. 159.3 и 159.6 УК РФ; п. «в» ч. 3 и ч. 5 ст. 222 УК РФ, ст. 222.1 и 222.2 УК РФ; п. «д» ч. 2 ст. 230 УК РФ; п. «г» ч. 2 ст. 242.2 УК РФ; ст. 272, 273, 274, 274.1 и 274.2 УК РФ.

К киберпреступлениям при наличии определенных условий отнесены, например: «использование сети “Интернет”, сети Даркнет, фишингового (поддельного) сайта или ссылки, средств мобильной связи, неправомерное списание денежных средств со счетов банковских карт, использование вредоносных компьютерных программ и другие» (Перечень № 25).

---

[11] Федеральный закон № 161-ФЗ от 27.06.2011 (последняя редакция). (2011). СПС «КонсультантПлюс».

[12] Приказ МВД России № 1110 от 29.12.2022. (Документ опубликован не был). СПС «КонсультантПлюс».

Можно отметить, что вторая группа преступлений сформирована по основаниям применения функционала ИТ для совершения преступлений. Например, функционал таких ИТ, как Интернет и телефонные коммуникации, позволяет формировать организованные преступные группы (Жарова, 2019) в целях совершения масштабного мошенничества и краж[13, 14].

Далее обратимся к статистическим данным по компьютерным преступлениям за период с января 2022 г. по сентябрь 2025 г.

2. Общая статистика по всем группам киберпреступлений за рассматриваемый период

Обозначенный временной отрезок выбран для оценки текущей ситуации и отображения последних тенденций. Анализу были подвергнуты статистические данные ГИАЦ МВД России о количестве преступлений[15]. Основное отличие структуризации указанных данных от Перечня № 25 заключается в порядке группировки.

По результатам расчетов получен график (рис. 1), отражающий месячные значения зарегистрированных дел по всем киберпреступлениям с января 2022 г. по сентябрь 2025 г.

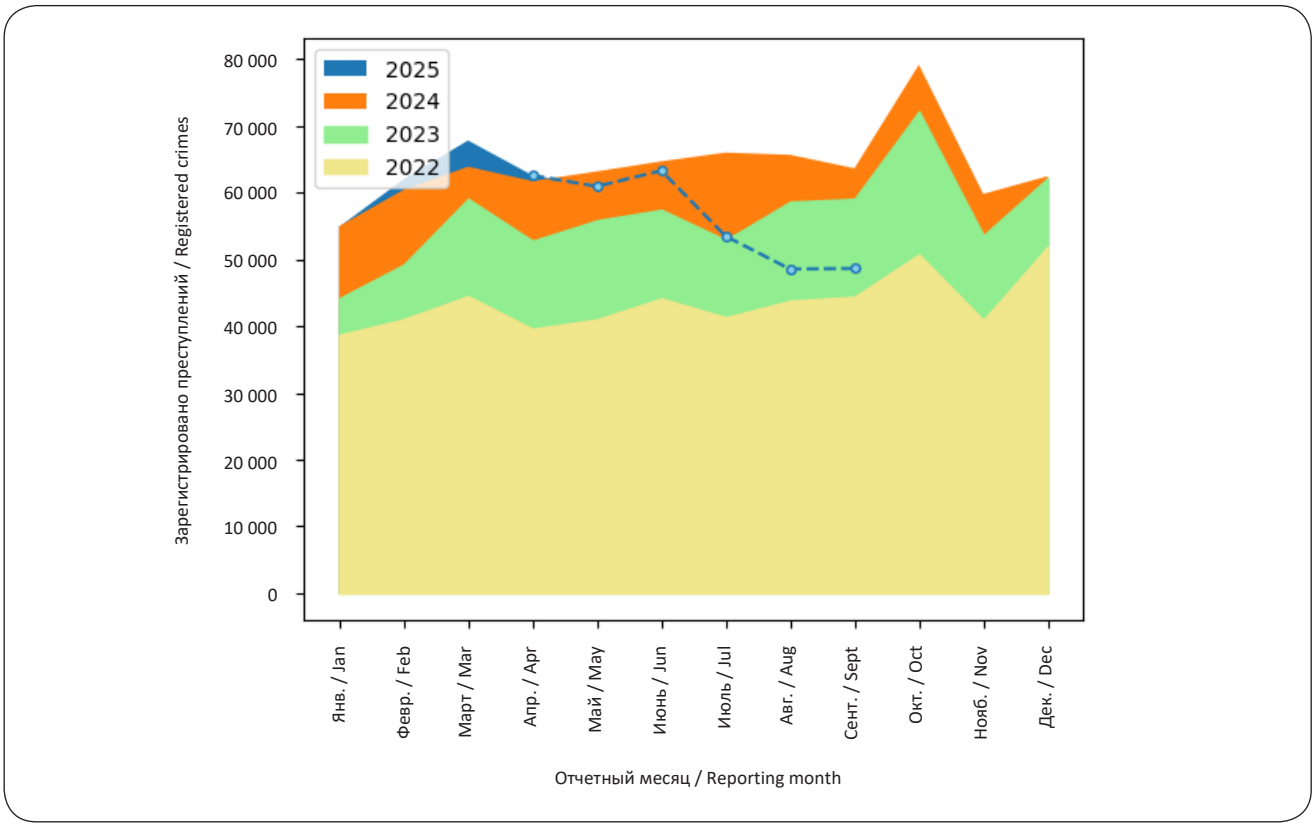

Рисунок 1. Динамика зарегистрированных киберпреступлений

Источник: составлено авторами по данным ГИАЦ МВД России[16].

Figure 1. Dynamics of registered cybercrimes

Source: compiled by the authors with the data of the Main Information and Analytical Center of the Russian Ministry of Internal Affairs[16].

[13] О вопросах противодействия преступности в сфере использования информационно-коммуникационных технологий. Администрация муниципального образования «Черняховский муниципальный округ Калининградской области». https://che.gov39.ru/poleznaya-informatsiya/10324/

[14] Постановление № 51-24 Межпарламентской Ассамблеи государств – участников СНГ. (2021). Информационный бюллетень. Межпарламентская Ассамблея государств – участников СНГ, 73 (Ч. 3).

[15] Состояние преступности. (2025, 24 декабря). Министерство внутренних дел Российской Федерации. https://мвд.рф/reports

[16] Там же.

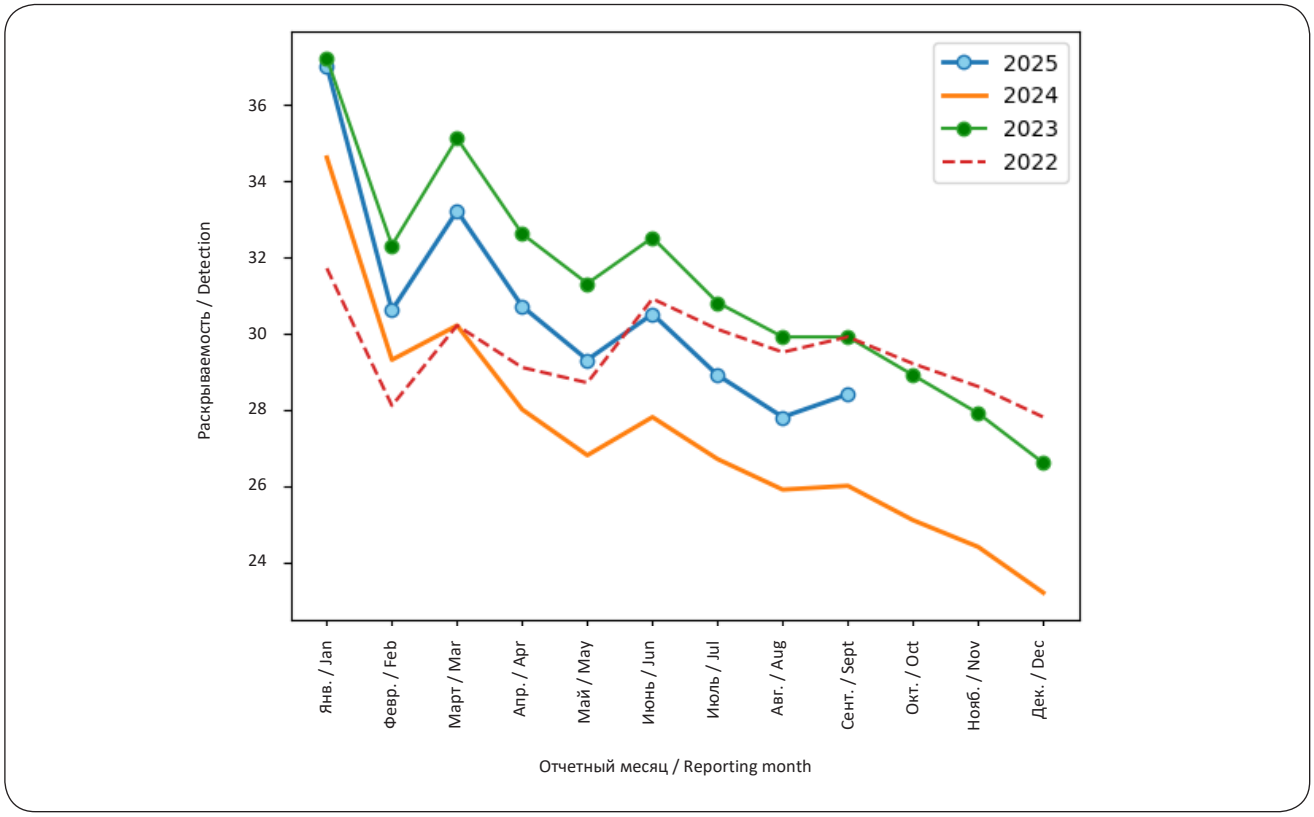

Рисунок 2. Динамика раскрываемости киберпреступлений

Источник: составлено авторами по данным ГИАЦ МВД России[17].

Figure 2. Dynamics of cybercrime clearance rate

Source: compiled by the authors with the data of the Main Information and Analytical Center of the Russian Ministry of Internal Affairs[17].

Данный график наглядно демонстрирует, что в 2023, 2024 гг. и в первый квартал 2025 г. число зарегистрированных киберпреступлений стабильно превышало численные показатели за тот же период предыдущих лет (рис. 1). В то же время период апрель – сентябрь 2025 г. принципиально не соответствует рамкам такой тенденции. В апреле, мае и июне 2025 г. (II квартале) значения зафиксированы на уровне 2024 г. – без увеличения количества. Далее в июле 2025 г. зарегистрировано киберпреступлений на уровне показателя 2023 г. со снижением их количества почти на 15 % по сравнению с июлем 2024 г. и июнем 2025 г. Затем в августе 2025 г. снижение усилилось – количество киберпреступлений почти на 24 % ниже, чем в заключительный месяц первого полугодия 2025 г. В сентябре 2025 г. регистрируемая киберпреступность сохранилась на уровне августа. Показатели августа – сентября 2025 г. ниже не только значений 2024-го, но и 2023 г.

Кроме того, в контексте предотвращения киберпреступлений важна статистика раскрытых киберпреступлений из рассмотренного количества зарегистрированных киберпреступлений.

На рис. 2 представлен график раскрываемости киберпреступлений правоохранительными органами на основании данных ГИАЦ МВД России.

Анализ полученных на графиках данных позволяет сделать вывод, что число киберпреступлений растет ежегодно. При этом количественные показатели раскрытых преступлений увеличиваются в январе каждого года. В январе традиционно фиксируется рост раскрываемости киберпреступлений. Например, по данным МВД России, в первом квартале 2023 г. раскрываемость киберпреступлений выросла до 35,1 %[18]. Это выше

[17] Состояние преступности. (2025, 24 декабря). Министерство внутренних дел Российской Федерации. https://мвд.рф/reports

[18] Статистические сведения о состоянии преступности в январе – марте 2023 г. (2023, 27 апреля). Пресс-центр МВД России. https://mvdmedia.ru/news/official/statisticheskie-svedeniya-o-sostoyanii-prestupnosti-v-yanvare-marte-2023-goda/

среднегодовых показателей, которые обычно колеблются в районе 25–30 %[19]. Возникает закономерный вопрос об объяснении данного наблюдения.

Во-первых, такая динамика объясняется тем, что в начале года органы внутренних дел подводят итоги предыдущего периода, формируют планы по раскрытию преступлений и работают с накопившимися нераскрытыми делами.

Во-вторых, часть дел, начатых в конце предыдущего года и оконченных расследованием в текущем году, направляются в суд. Статистическая учетность ведется в соответствии с приказом Генпрокуратуры России № 39, МВД России № 1070, МЧС России № 1021, Минюста России № 253, ФСБ России № 780, Минэкономразвития России № 353, ФСКН России № 399 от 29.12.2005 (ред. от 15.10.2019) «О едином учете преступлений»[20]. Это связано с особенностями процессуального учета: многие преступления, совершенные в декабре, попадают в январскую статистику, поскольку расследование занимает длительное время.

В-третьих, в январе фиксируется относительное снижение числа новых преступлений в других группах (например, уличных разбоев, краж и т. д.), что позволяет перераспределить ресурсы на расследование киберпреступлений[21]. Кроме того, в этот период снижается активность самих преступников из-за праздничных дней, что облегчает работу следственных органов. Однако, несмотря на положительную динамику по отдельным показателям, общий уровень раскрываемости остается относительно низким из-за сложности расследования компьютерных инцидентов.

На раскрываемость влияет также и усиление противодействия киберпреступлениям со стороны МВД и других ведомств, и это сказывается на статистике. Так, в целях усиления противодействия правонарушениям и преступлениям в 2022 г. было создано подразделение полиции в составе МВД России – Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий[22].

Кроме того, 1 июня 2025 г. вступил в силу, за исключением отдельных положений, Федеральный закон «О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации»[23] (далее – ГИС «П-ИКТП»). Допустимо отметить, что начиная с июля 2025 г. наблюдалось снижение количества зарегистрированных киберпреступлений, которое может являться эффектом от начала функционирования созданной ГИС «П-ИКТП». Для проверки отмеченной гипотезы авторы продолжат работу по отслеживанию динамики количества регистрируемых киберпреступлений, особенно по итогам полноценного запуска ГИС «П-ИКТП» в марте 2026 г.[24]

Эти изменения демонстрируют совершенствование организационно-правовых и технических мер, направленных на противодействие киберпреступлениям, а также на оперативное предупреждение, выявление и пресечение правонарушений и преступлений, совершаемых с использованием информационных и телекоммуникационных технологий, организации взаимодействия органов и организаций.

В то же время полученный рост раскрываемости компьютерных преступлений в январе обусловлен сочетанием организационных, процессуальных и сезонных факторов: активизацией работы правоохранитель-

---

[19] МВД России публикует статистические данные о состоянии преступности в РФ за восемь месяцев 2023 г. (2023, 22 сентября). Пресс-центр МВД России. https://mvdmedia.ru/news/official/mvd-rossii-publikuet-statisticheskie-dannye-o-sostoyanii-prestupnosti-v-rossiyskoy-federatsii-za-vos/

[20] Приказ Генпрокуратуры России № 39, МВД России № 1070, МЧС России № 1021, Минюста России № 253, ФСБ России № 780, Минэкономразвития России № 353, ФСКН России № 399 от 29.12.2005 (ред. от 15.10.2019) «О едином учете преступлений» (вместе с «Типовым положением о едином порядке организации приема, регистрации и проверки сообщений о преступлениях», «Положением о едином порядке регистрации уголовных дел и учета преступлений», «Инструкцией о порядке заполнения и представления учетных документов»). (2006). Российская газета, 13.

[21] В РФ в 2023 г. почти на 30 % больше зарегистрировано IT-преступлений. (2024, 8 февраля). Информационное агентство ТАСС. https://tass.ru/ekonomika/19934623

[22] Указ Президента РФ № 688 от 30.09.2022. (2022). СЗ РФ, 40, ст. 6787.

[23] Федеральный закон № 41-ФЗ от 01.04.2025. (2025). СЗ РФ, 14, ст. 1574.

[24] ГИС противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий. (2025, 12 мая). TAdviser. https://www.tadviser.ru/index.php/Статья:ГИС_противодействия_правонарушениям,_совершаемым_с_использованием_информационных_и_коммуникационных_технологий

ных органов, завершением дел, перенесенных с предыдущего года, особенностями статистического учета и перераспределением ресурсов в условиях снижения других видов преступности.

Но картина киберпреступности не будет полной без представления индикатора равновесия между защитой прав человека и эффективностью противодействия преступности, как соотношения оправданных и осужденных. Для этого проведем анализ данных о количестве оправданных или осужденных по статьям УК РФ за год, относящихся к группе киберпреступлений без дополнительных условий в соответствии с Перечнем № 25. Поскольку не все данные представлены в материалах ГИАЦ МВД России, авторы обратились к аналитическим материалам Агентства правовой информации[25] и TAdviser.

3. Анализ данных о количестве оправданных или осужденных за год по статьям УК РФ, которые относятся к группе киберпреступлений без дополнительных условий

Анализу подлежали показатели количества оправданных или осужденных за период с января 2022 г. по декабрь 2024 г., данные за 2025 г. отсутствуют по причине их представления в рассматриваемых источниках за полный год, а не по месяцам или кварталам.

В первой части данного раздела статьи исследуются данные о совершенных киберпреступлениях без дополнительных условий: ст. 159.3, 159.6, 272, 273, 274, 274.1, 274.2 УК РФ.

Во второй части данного раздела анализируются данные о киберпреступлениях без дополнительных условий, квалифицируемые по ч. 3 ст. 158 УК РФ; ч. 3, 5 ст. 222, 222.1, 222.2 УК РФ; ч. 2 ст. 230 УК РФ; ч. 2 ст. 242.2 УК РФ, без рассмотрения данных по пунктам частей, поскольку подобная детализированная информация не обнаружена в открытых источниках.

3.1. Анализ данных по киберпреступлениям без дополнительных условий: ст. 159.3, 159.6, 272, 273, 274, 274.1, 274.2 УК РФ

Количественные показатели осужденных и оправданных по преступлениям, предусмотренным ст. 159.3, 159.6, 272, 273, 274, 274.1 и 274.2 УК РФ за 2022–2024 гг., представлены в табл. 1. Источником данных послужили материалы Агентства правовой информации.

Таблица 1. Количественные показатели осужденных по киберпреступлениям без дополнительных условий
Table 1. Quantitative indicators of the convicted for cybercrimes without additional conditions

Статья УК РФ* / Article CC RF*	Год / Year					
	2022		2023		2024	
	Оправдано / Acquitted	Осуждено / Convicted	Оправдано / Acquitted	Осуждено / Convicted	Оправдано / Acquitted	Осуждено / Convicted
159.3	0	113	0	78	1	35
159.6	0	29	0	15	0	17
272	1	179	0	221	0	267
273	0	46	0	32	0	35
274	0	1	0	1	0	1
274.1	0	54	0	79	0	77
274.2	Включена в УК РФ 14 июля 2022 г. Данные не представлены / Added to CC RF on 14 July 2022. No data available		0	0	0	0

* *CC RF* – Criminal Code of the Russian Federation.

[25] Уголовное судопроизводство. Данные о назначенном наказании по статьям УК РФ. Агентство правовой информации. https://stat.апи-пресс.рф/stats/ug/t/14/s/17

Итак, анализ данных позволяет сделать следующий вывод: показатели дел, завершившихся оправдательным приговором, не дают полной картины, поскольку редки. Показатели количества осужденных за преступления в сфере компьютерной информации: ст. 272, 274.1 УК РФ – продемонстрирован рост; по ст. 273 УК РФ – фактически остались прежними; по ст. 274 УК РФ – зафиксированы единичные случаи.

В свою очередь, за мошенничество с использованием электронных средств платежа и в сфере компьютерной информации – ст. 159.3, 159.6 УК РФ – зафиксировано снижение количества осужденных в 2023–2024 гг. по сравнению с 2022 г.

В целях визуализации полученного результата покажем динамику осужденных на графиках (рис. 3). Но при этом из рассматриваемых данных авторами исключены значения оправданных, а также значения, соответствующие ст. 274.2 УК РФ, ввиду их единичных случаев.

3.2. Анализ показателей киберпреступлений без дополнительных условий: ч. 3 ст. 158; ч. 3, 5 ст. 222, 222.1, 222.2; ч. 2 ст. 230, ч. 2 ст. 242.2 УК РФ

Несмотря на то, что к киберпреступлениям без дополнительных условий в Перечне № 25 отнесены п. «г» ч. 3 ст. 158; п. «в» ч. 3, 5 ст. 222, 222.1, 222.2; п. «д» ч. 2 ст. 230, п. «г» ч. 2 ст. 242.2, авторы статьи были вынуждены рассматривать менее детализированную информацию по данным статьям, поскольку анализ доступной статистической информации показывает, что детализированные данные о привлечении к уголовной ответственности по конкретным пунктам частей вышеуказанных статей УК РФ в открытом доступе практически отсутствуют.

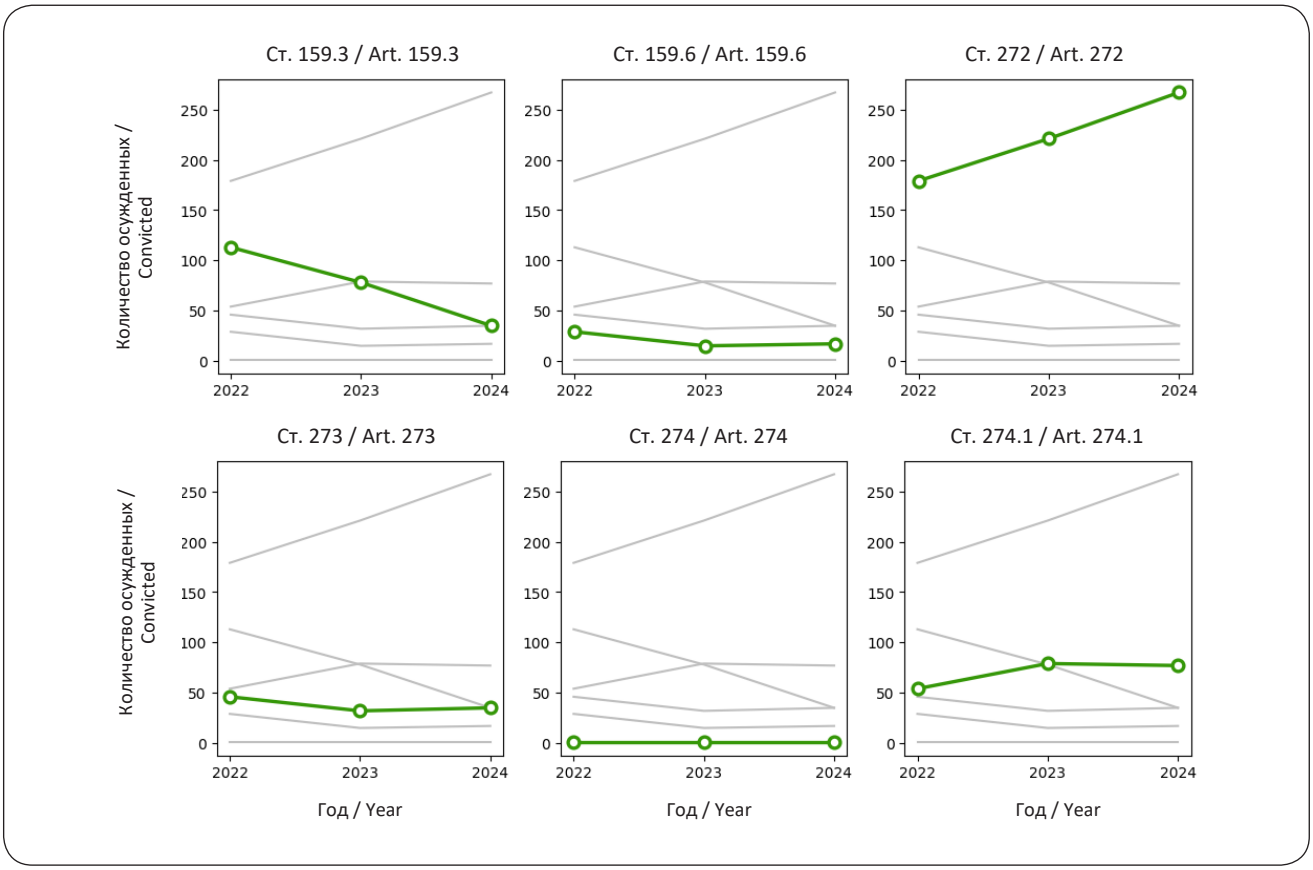

Рисунок 3. Динамика количества осужденных по ряду статей киберпреступлений без дополнительных условий

Источник: составлено авторами по данным Агентства правовой информации.

Figure 3. Dynamics of the number of convicts under certain cybercrime articles without additional conditions

Source: compiled by the authors according to the data of the Agency for Legal Information.

Кроме того, официальная судебная статистика традиционно публикуется в агрегированном виде по статьям в целом, что затрудняет получение точных данных по конкретным пунктам частей статей УК РФ. Это ограничение связано с методологией формирования статистической отчетности, которая не предусматривает выделение квалифицированных составов преступлений в отдельные группы.

Статья 222 УК РФ

Анализ судебных решений показывает, что применение п. «в» ч. 3 ст. 222 УК РФ становится все более актуальным в условиях цифровизации общества. Преступления, связанные с незаконным оборотом оружия, совершаемые с использованием Интернета, характеризуются высокой латентностью и сложностью выявления[26]. Несмотря на это, статистика показывает, что в 2024 г. количество преступлений, связанных с незаконным приобретением, передачей, сбытом, хранением, перевозкой, пересылкой или ношением оружия, его основных частей и боеприпасов, снизилось на 5,4 %. Всего было выявлено 8 384 таких случая, что меньше, чем в 2023 г.

Статья 222.1 УК РФ

Существенные изменения в статью 222.1 УК РФ были внесены Федеральным законом № 281-ФЗ[27], которые привели к ужесточению ответственности. Эти изменения отразились на характере рассмотрения дел судами. В частности, Конституционный суд РФ в Постановлении от 13 ноября 2023 г. № 52-П рассматривал вопросы конституционности отдельных положений ст. 222.1 УК РФ[28], что свидетельствует о продолжающемся процессе совершенствования правового регулирования в данной сфере.

В то же время статистические данные демонстрируют устойчивую тенденцию увеличения числа лиц, привлекаемых к уголовной ответственности по ст. 222.1 УК РФ. Согласно данным судебной статистики, количество осужденных по этой статье возросло. В 2023 г. по ст. 222.1 УК РФ были осуждены 2 325 человек, что на 19,4 % больше по сравнению с 2022 г., когда число осужденных составляло 1 948 человек. Количество выявленных фактов хищения и вымогательства взрывчатых веществ и взрывных устройств в 2024 г., по сравнению с 2023 г., сократилось на 6,2 % (542 преступления).

Статья 222.2 УК РФ

Количество выявленных преступлений, связанных с незаконным оборотом оружия, в 2024 г., по сравнению с 2023 г., сократилось на 4,2 % и составило 18,6 тыс., а количество выявленных фактов хищения и вымогательства оружия, боеприпасов, взрывчатых веществ и взрывных устройств сократилось на 6,2 % (542 преступления).

Несмотря на общее снижение числа преступлений, фиксируется рост доли дел с отягчающими обстоятельствами, в том числе с использованием ИТ и участием организованных групп. Четыре преступления из пяти (84,8 %) совершаются с использованием Интернета (649,1 тыс.; +23,2 %), почти половина (45,2 %) – средств мобильной связи (346,0 тыс.; +14,3 %).

Статья 158 УК РФ

В 2024 г. наибольшее число граждан осуждено за совершение преступлений против собственности, как и годом ранее[29]. С 2018 г. в ч. 3 добавлен пункт «г» – кража с банковского счета или электронных денежных средств. В последние годы фиксируется рост числа таких преступлений, что связано с цифровизацией финансовой сферы и увеличением числа безналичных операций. По делам о кражах сохраняется высокая доля осужденных – 73 %, по итогам 2024 г., при крайне низком проценте оправданий[30]. Большая часть дел рассматривается в особом порядке (29 %), что свидетельствует о признании вины и заключении досудебных соглашений.

Статья 230 УК РФ

За 2021–2023 гг. были внесены важные изменения в ст. 230 УК РФ, усилившие ответственность за склонение к потреблению наркотиков, включены квалифицирующие признаки – использование информационно-телекоммуникационной сети, например Интернета. В 2024 г. практика применения статьи смещается в сторону

---

[26] Преступность в России. (2025, 22 декабря). TAdviser. https://www.tadviser.ru/index.php/Статья:Преступность_в_России

[27] Федеральный закон № 281-ФЗ от 01.07.2021. (2021). СЗ РФ, 27 (Ч. I), ст. 5109.

[28] Постановление КС РФ № 52-П от 13.11.2023. (2023). СЗ РФ, 48, ст. 8655.

[29] Опубликована статистика состояния судимости за 2024 г. (2025, 14 мая). Адвокатская газета. https://www.advgazeta.ru/obzory-i-analitika/opublikovana-statistika-sostoyaniya-sudimosti-za-2024-g/

[30] Уголовное судопроизводство. Общие показатели по категориям дел. Агентство правовой информации. https://stat.апи-пресс.рф/stats/ug/t/11/s/1

ужесточения наказаний по квалифицированным составам, особенно в случаях, связанных с несовершеннолетними и использованием цифровых технологий для склонения к совершению преступления[31].

В официальных отчетах за 2024 г. отмечается, что преступления, связанные с незаконным оборотом наркотиков, остаются на высоком уровне. Так, за январь – декабрь 2024 г. выявлено 198 тыс. преступлений, связанных с незаконным оборотом наркотиков, что на 3,7 % больше, чем за аналогичный период 2023 г. При этом сотрудниками органов внутренних дел выявлено 191,8 тыс. преступлений (+3,3 %). По сравнению с январем – декабрем 2023 г. на 7,0 % увеличилось число выявленных преступлений, совершенных с целью сбыта наркотических средств, психотропных веществ или их аналогов. Также увеличился их удельный вес в числе преступлений, связанных с незаконным оборотом наркотиков, с 66,1 % в январе – декабре 2023 г. до 68,2 %.

Статья 242 УК РФ

По данным ГИАЦ МВД России, число зарегистрированных преступлений совокупно по ст. 242, 242.1, 242.2 УК РФ составляет 3 554, что на 13,7 % выше, чем в 2023 г. Однако, согласно данным Единой межведомственной информационно-статистической системы (ЕМИСС), по ст. 242 УК РФ в последние годы фиксируется относительно стабильное количество зарегистрированных преступлений, без резких скачков вверх или вниз[32].

Сведения по ч. 3 ст. 158 УК РФ представлены на отдельном графике по причине различных порядков соответствующих значений, что при объединении в рамках одного рисунка привело бы к искажениям масштаба.

Анализ данных о числе осужденных за киберпреступления по вышеперечисленным статьям позволяет сделать вывод, что фактически по всем частям этих статей усредненные показатели за три года остаются на одном уровне. Исключением стали ч. 5 ст. 222 и ч. 3 ст. 222.1: по ним наблюдается устойчивый рост числа осужденных, а также ч. 3 ст. 158 УК РФ, по которой зафиксировано снижение количества осужденных в 2024 г. Хотя в СМИ можно встретить иную точку зрения относительно ч. 3 ст. 222.1 УК РФ. Так, «около 80 % осужденных по статье 222.1 УК РФ получают условное наказание, в то время как одна пятая часть приговаривается к реальным срокам лишения свободы»[33]. Данные ч. 3, 5 ст. 222.2 УК РФ не показательны в контексте осужденных, поскольку за три года зафиксирован единичный случай.

Таблица 2. Данные о количестве осужденных и оправданных по киберпреступлениям без дополнительных условий: ч. 3 ст. 158 УК РФ; ч. 3,5 ст. 222, 222.1, 222.2 УК РФ; ч. 2. ст. 230 УК РФ; ч. 2 ст. 242.2 УК РФ

Table 2. Data on the number of persons convicted and acquitted of cybercrime without additional conditions: Part 3 of Article 158 of the Russian Criminal Code; Parts 3, 5 of Articles 222, 222.1, 222.2 of the Russian Criminal Code; Part 2 of Article 230 of the Russian Criminal Code; Part 2 of Article 242.2 of the Russian Criminal Code

Статья УК РФ / Article CC RF	Год / Year					
	2022		2023		2024	
	Оправдано / Acquitted	Осуждено / Convicted	Оправдано / Acquitted	Осуждено / Convicted	Оправдано / Acquitted	Осуждено / Convicted
Ч. 3 ст. 158 / Part 3 of Art. 158	8	54 399	11	53 536	11	45 846
Ч. 3 ст. 222 / Part 3 of Art. 222	0	30	0	31	1	27
Ч. 5 ст. 222 / Part 5 of Art. 222	0	14	0	31	0	58
Ч. 3 ст. 222.1 / Part 3 of Art. 222.1	0	1	0	18	0	25
Ч. 5 ст. 222.1 / Part 5 of Art. 222.1	0	10	0	25	0	20
Ч. 3 ст. 222.2 / Part 3 of Art. 222.2	0	0	0	0	0	0
Ч. 5 ст. 222.2 / Part 5 of Art. 222.2	0	0	0	0	0	1
Ч. 2 ст. 230 / Part 2 of Art. 230	0	8	0	9	0	6
Ч. 2 ст. 242.2 / Part 2 of Art. 242.2	0	19	0	30	0	25

[31] Уголовная ответственность за склонение к потреблению наркотиков с использованием сети Интернет. (2024, 3 декабря). Пресс-служба прокуратуры г. Нижневартовска. https://www.n-vartovsk.ru/news/citywide_news/bgorod/prokuratura_informiruet/490200.html

[32] Количество преступлений, зарегистрированных в отчетном периоде. ЕМИСС. https://www.fedstat.ru/indicator/36225

[33] В России число осужденных за изготовление взрывчатки возросло в шесть раз за три года. (2018, 21 апреля). Информационное агентство ТАСС. https://tass.ru/politika/5147146

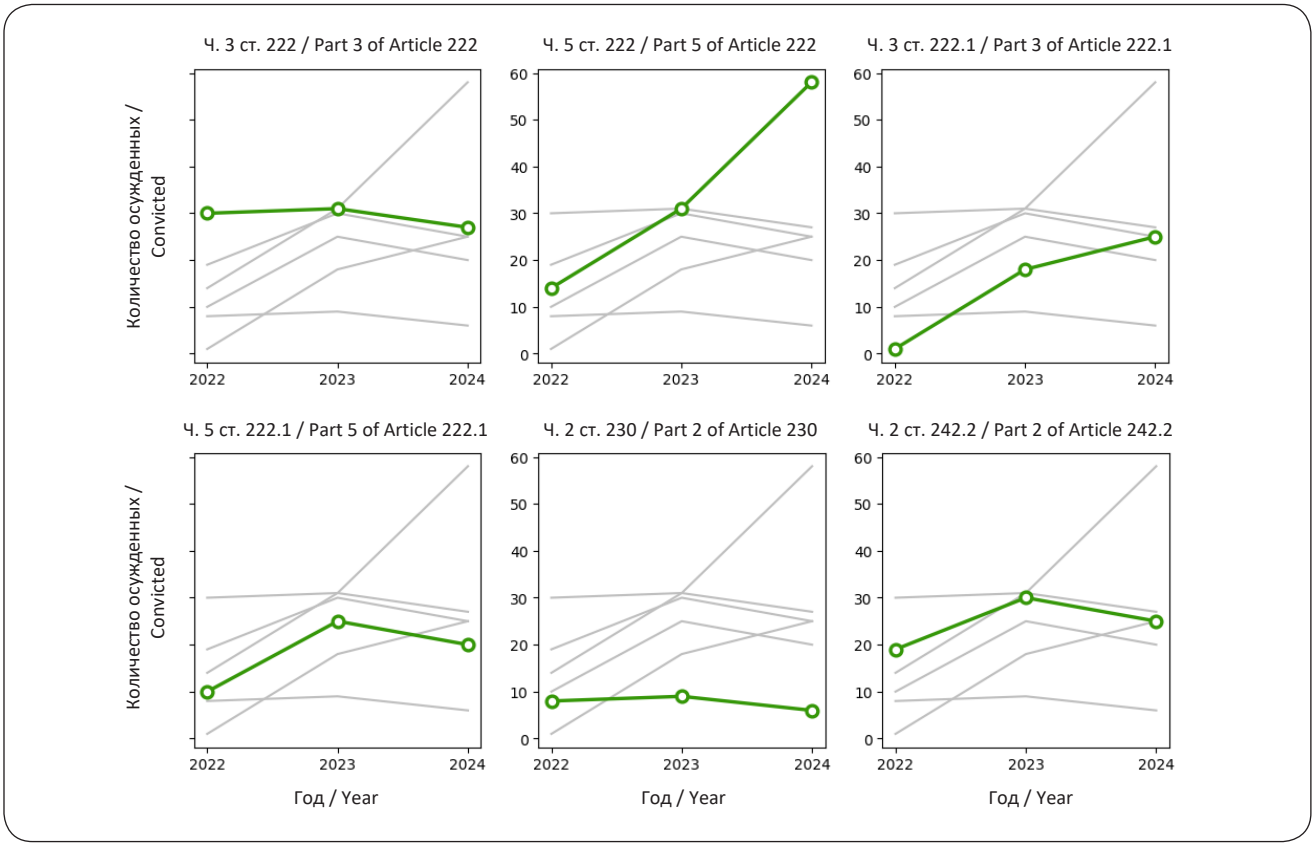

Рисунок 4. Динамика количества осужденных по ряду статей: ч. 3, 5 ст. 222, 222.1 УК РФ; ч. 2. ст. 230 УК РФ, ч. 2 ст. 242.2 УК РФ

Источник: составлено авторами по данным Агентства правовой информации.

Figure 4. Dynamics of the number of convicts under certain articles: Parts 3, 5 of Articles 222, 222.1 of the Russian Criminal Code; Part 2 of Article 230 of the Russian Criminal Code, Part 2 of Article 242.2 of the Russian Criminal Code

Source: compiled by the authors according to the data of the Agency for Legal Information.

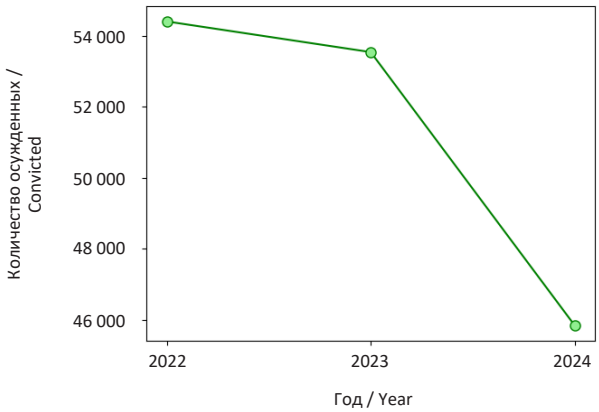

Рисунок 5. Динамика количества осужденных по ч. 3 ст. 158 УК РФ

Источник: составлено авторами по данным Агентства правовой информации.

Figure 5. Dynamics of the number of convicts under Part 3 of Article 158 of the Russian Criminal Code

Source: compiled by the authors according to the data of the Agency for Legal Information.

Для визуализации представленных данных, аналогично предыдущему подразделу, покажем динамику осужденных на графиках (рис. 4, 5). Из рассматриваемых данных авторами исключены значения оправданных, а также значения, соответствующие ч. 3, 5 ст. 222.2 УК РФ, ввиду их единичных случаев.

С нашей точки зрения, результат, полученный на основании анализа данных, представленных ГИАЦ МВД России и Агентством правовой информации (раздел судебной статистики), в очередной раз показывает, что Интернет и другие информационные технологии помогают создавать организованные преступные группы для совершения тяжких преступлений. В то же время статистика показывает сложность фиксации и выявления киберпреступлений.

Заключение

Подводя итог проведенному исследованию, авторы отмечают следующее. Несмотря на общее снижение числа преступлений, фиксируется ежегодный рост числа киберпреступлений, в частности, с отягчающими обстоятельствами, в том числе с использованием Интернета, мессенджеров и участием организованных групп. В связи с широким спектром киберпреступлений Генпрокуратура России и МВД России разработали перечень, разделив преступления на две группы: преступления, относящиеся к перечню без дополнительных условий, и преступления, относящиеся к перечню при наличии определенных условий.

Анализ статистических данных за 2022–2025 гг. по числу зарегистрированных киберпреступлений позволил выявить следующие закономерности. В первый квартал 2025 г. и на протяжении полных 2023 и 2024 гг. наблюдалось устойчивое повышение количества киберпреступлений в сравнении с численными показателями за тот же период предыдущих годов. При этом показатели раскрываемости преступлений являются ежегодно высокими в январе каждого года. Объяснить это можно сочетанием организационных, процессуальных и сезонных факторов: активизацией работы правоохранительных органов; особенностями статистического учета и перераспределением ресурсов в условиях снижения других видов преступности. Позитивными наблюдениями стали незначительное замедление роста количества киберпреступлений во втором квартале 2025 г. (показатели на уровне II квартала 2024 г.), а также значительное их снижение в третьем квартале 2025 г. (–15 % в июле 2025 г. и почти –24 % в августе – сентябре по сравнению с июнем 2025 г.). Сказать о переломе тенденции роста количества киберпреступлений на основании лишь шести месяцев рано – необходим больший горизонт фиксации подобных значений. Однако этого достаточно, чтобы говорить о наличии сигнала в пользу скорого перелома в тенденции роста количества киберпреступлений. Заметим, что период снижения совпал со вступлением в силу изменений в федеральном законодательстве, закрепивших основы создания и функционирования Государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий.

Сравнение соотношения оправданных и осужденных по преступлениям, относящимся к перечню без дополнительных условий (ст. 159.3, 159.6, 272, 273, 274, 274.1, 274.2 УК РФ), за 2022–2024 гг. позволило сделать следующий вывод. Показатели дел, завершившихся оправдательным приговором, не дают полной картины, поскольку такой исход дела представлен незначительным количеством или единичными случаями.

Показатели количества осужденных за преступления в сфере компьютерной информации по ст. 272 УК РФ показали устойчивый рост от года к году. Также наблюдается незначительный рост числа осужденных по ст. 274.1 УК РФ, в особенности при сравнении с уровнем 2022 г. По прочим статьям: 273–274 и 274.2 гл. 28 УК РФ – динамика количества осужденных не показала существенных изменений. В свою очередь, в 2023–2024 гг. по сравнению с 2022 г. зафиксировано снижение количества осужденных за мошенничество с использованием электронных средств платежа или в сфере компьютерной информации.

Относительно ряда других статей Перечня № 25 (ч. 3 ст. 158; ч. 3, 5 ст. 222, 222.1; ч. 2 ст. 230; ч. 2 ст. 242.2 УК РФ) в части динамики числа осужденных допустимо отметить следующее. 2024 год охарактеризовался значительным снижением количества осужденных за кражи, совершенные с незаконным проникновением в жилище; из нефте- или газопроводов; в крупном размере; с банковского счета или в отношении электронных денежных средств – около –14,4 %. Статистика осужденных по ч. 3, 5 ст. 222.2 УК РФ не предоставляет возможности определить динамику последних трех лет по причине единичного случая назначенного наказания. Часть 3 ст. 222 УК РФ и ч. 2 ст. 230 УК РФ отличаются отсутствием значимых изменений количества осужденных. Количество осужденных в 2023–2024 гг. по ч. 5 ст. 222.1 УК РФ и ч. 2 ст. 242.2 УК РФ

увеличилось по сравнению с 2022 г. В свою очередь, наблюдается устойчивый рост от года к году количества осужденных за преступления, квалифицируемые ч. 5 ст. 222 УК РФ, а также ч. 3 ст. 222.1 УК РФ.

Рост числа зарегистрированных киберпреступлений при сохранении низкого уровня их раскрываемости указывает на сложность выявления преступлений, совершаемых с использованием ИТ и информации. Одним из шагов решения данной проблемы является созданная государственная информационная система противодействия правонарушениям, совершаемым с использованием ИТ. Но это только начало. В дальнейшем необходимо продолжить формирование системы организационно-правовых и технических мер противодействия киберпреступлениям. Например, создается специализированная цифровая платформа для оперативного обмена информацией между правоохранительными органами, Центральным банком, кредитными организациями и операторами связи. Такая платформа позволит не только ускорить обмен сведениями о киберпреступлениях, но и обеспечит возможность оперативной приостановки подозрительных финансовых операций и блокировки мошеннических переводов. Для проактивного предотвращения киберпреступлений в целом должны применяться системы искусственного интеллекта и аналитики больших данных, которые помогут в прогнозировании и предотвращении преступлений в цифровой среде.

Авторы с осторожным оптимизмом выражают уверенность, что зафиксированное во II–III кварталах 2025 г. снижение киберпреступности – не просто статистическое отклонение в тенденции, а сигнал скорого перелома тенденции ее роста.

Список литературы

Агравал, А. (2023). Киберпреступления, связанные с электронными картами, и банковское мошенничество. *Право и цифровая экономика*, *1*, 60–71. EDN: SANSOJ. DOI: 10.17803/2618-8198.2023.19.1.060-071

Баранов, А. А., Соломатина, Е. А. (2023). К вопросу о способах совершения преступлений с использованием информационно-телекоммуникационных технологий. *Криминологический журнал*, *3*, 26–30. EDN: SSTPBV. DOI: 10.24412/2687-0185-2023-3-26-30

Быкова, Е. Г., Казаков, А. А. (2024). Дискуссионные аспекты признания электронных средств и электронных носителей информации предметом преступления, предусмотренного ст. 187 УК РФ. *Российский судья*, *4*, 13–18. EDN: JOWNML. DOI: 10.18572/1812-3791-2024-4-13-18

Евдокимов, К. Н. (2025). К вопросу совершенствования квалификации преступлений в сфере компьютерной информации (по материалам судебной практики). *Российский судья*, *2*, 36–40. EDN: KXUHGR. DOI: 10.18572/1812-3791-2025-2-36-40

Елин, В. М. (2022). О подходах к криминологической характеристике лиц, совершающих преступления в сфере компьютерной информации. *Российский следователь*, *7*, 61–65. EDN: ASGYIM. DOI: 10.18572/1812-3783-2022-7-61-65

Елин, В. М., Жарова, А. К. (2009). О выделении информационных объектов в самостоятельную категорию объекта преступления. *Труды Института государства и права Российской академии наук*, *5*, 205–229. EDN: SAMBAN

Жарова, А. К. (2019). Маршрутизация и IP для обеспечения правового регулирования интернет-отношений. *Вестник РГГУ. Серия: Информатика. Информационная безопасность. Математика*, *2*, 32–42. EDN: LGLHKL. DOI: 10.28995/2686-679X-2019-2-32-42

Жарова, А. К. (2023a). Достижение алгоритмической прозрачности и управление рисками информационной безопасности при принятии решений без вмешательства человека: правовые подходы. *Journal of Digital Technologies and Law*, *1*(4), 973–993. EDN: OPPOBG. DOI: 10.21202/jdtl.2023.42

Жарова, А. К. (2023b). Искусственный интеллект – средство или способ совершения мошенничества в сфере компьютерной информации? *Государство и право*, *2*, 54–61. EDN: PESJQJ. DOI: 10.31857/S102694520021177-5

Жмуров, Д. В. (2024). Показатели преступности в сфере информационно-телекоммуникационных технологий в 2019–2023 годах (виктимологический аспект). *Российский судья*, *5*, 19–23. EDN: FFQFTY. DOI: 10.18572/1812-3791-2024-5-19-23

Курушин, В. Д., Минаев, В. А. (1998). *Компьютерные преступления и информационная безопасность*. Москва: Новый юрист. EDN: PXOOXP

Россинская, Е. Р. (2021). Концепция учения об информационно-компьютерных криминалистических моделях как основе методик расследования компьютерных преступлений. *Вестник Восточно-Сибирского института МВД России*, *2*, 190–200. EDN: VLMMEC. DOI: 10.24412/2312-3184-2021-2-190-200

Русскевич, Е. А. (2025). О совокупности преступлений в сфере компьютерной информации с другими преступлениями. *Уголовное право*, *4*, 76–84. EDN: RSMKOS. DOI: 10.52390/20715870_2025_4_76

Унукович, А. С. (2021). Понятие преступлений, совершаемых с использованием информационно-телекоммуникационных технологий. *Государственная служба и кадры*, *4*, 278–280. EDN: GIKTGY. DOI: 10.24411/2312-0444-2021-4-278-280

Язов, Ю. К. (2025). Об определении понятия «кибербезопасность» и связанных с ним терминов. *Вопросы кибербезопасности*, *65*(1), 2–6. EDN: HNKWDB. DOI: 10.21681/2311-3456-2025-1-2-6

Alnakeep, H. T. (2022). Internet crimes to legal regulation. *International Journal of Health Sciences*, Online First, 48856–48876. EDN: FBVXYE. DOI: 10.53730/ijhs.v6ns7.13683

Al Makhmari, M., Al-Hammouri, A., Al-Billeh, T., & Almamari, A. (2024). Criminal Liability for Misuse of Social Media in Omani and UAE Legislation. *International Journal of Cyber Criminology*, *18*(2), 92–106. https://doi.org/10.5281/zenodo.476618206

Al Nagrash, A., Alareed, N., Aldulaimi, S., Abdeldayem, M., & Aswad, A. R. (2024). Unveiling the Legal Implications of regulating information technology crimes in violations of the social insurance law. *2024 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS)*, Manama, Bahrain, (pp. 39–47). https://doi.org/10.1109/icetsis61505.2024.10459364

Azhibayev, M. G., & Dzhanadilov, O. M. (2018). Cybercrime as a modern threat to military security. *Journal of Advanced Research in Law and Economics*, *9*(5), 1551–1557. EDN: VUOHTR. DOI: 10.14505//jarle.v9.5(35).06

Dremliuga, R., Dremliuga, O., & Kuznetsov, P. (2020). Combating the threats of cybercrimes in Russia evolution of the cybercrime laws and social concern. *Communist and Post-Communist Studies*, *53*(3), 123–136. EDN: GMJXAO. DOI: 10.1525/cpcs.2020.53.3.123

Onwuadiamu, G. (2025). Cybercrime in criminology; A systematic review of criminological theories, methods, and concepts. *Journal of Economic Criminology*, *8*(100136), 1–10. EDN: HHMEHI. DOI: 10.1016/j.jeconc.2025.100136

Sarkar, G., & Shukla, S. K. (2023). Behavioral analysis of cybercrime: Paving the way for effective policing strategies. *Journal of Economic Criminology*, *2*(100034), 1–26. EDN: RWRHGS. DOI: 10.1016/j.jeconc.2023.100034

Shukan, A., Abdizhami, A., Ospanova, G., & Abdakimova D. (2019). Crime control in the sphere of information technologies in the Republic of Turkey. *Digital Investigation*, 30, 94–100. EDN: NSDCPP. DOI: 10.1016/j.diin.2019.07.005

Younies, H., & Al-Tawil, T. N. (2020). Effect of cybercrime laws on protecting citizens and businesses in the United Arab Emirates (UAE). *Journal of Financial Crime*, *27*(4), 1089–1105. EDN: LCQMTW. DOI: 10.1108/JFC-04-2020-0055

References

Agrawal, A. (2023). Cybercrime with a particular focus on electronic cards and bank fraud. *Law and Digital Economy*, *1*, 60–71. (In Russ.). https://doi.org/10.17803/2618-8198.2023.19.1.060-071

Alnakeep, H. T. (2022). Internet crimes to legal regulation. *International Journal of Health Sciences*, Online First, 48856–48876. https://doi.org/10.53730/ijhs.v6ns7.13683

Al Makhmari, M., Al-Hammouri, A., Al-Billeh, T., & Almamari, A. (2024). Criminal Liability for Misuse of Social Media in Omani and UAE Legislation. *International Journal of Cyber Criminology*, *18*(2), 92–106. https://doi.org/10.5281/zenodo.476618206

Al Nagrash, A., Alareed, N., Aldulaimi, S., Abdeldayem, M., & Aswad, A. R. (2024). Unveiling the Legal Implications of regulating information technology crimes in violations of the social insurance law. *2024 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS)*, Manama, Bahrain, (pp. 39–47). https://doi.org/10.1109/icetsis61505.2024.10459364

Azhibayev, M. G., & Dzhanadilov, O. M. (2018). Cybercrime as a modern threat to military security. *Journal of Advanced Research in Law and Economics*, *9*(5), 1551–1557. https://doi.org/10.14505//jarle.v9.5(35).06

Baranov, A. A., & Solomatina, E. A. (2023). On the issue of ways of committing crimes using information and telecommunication technologies. *Criminological Journal*, *3*, 26–30. https://doi.org/10.24412/2687-0185-2023-3-26-30

Bykova, E. G., & Kazakov, A. A. (2024). Discussion aspects of acknowledgment of electronic means and electronic data storage devices as a subject of a crime stipulated by art. 187 of the Criminal Code of the Russian Federation. *Rossiyskiy sudya*, *4*, 13–18. (In Russ.). https://doi.org/10.18572/1812-3791-2024-4-13-18

Dremliuga, R., Dremliuga, O., & Kuznetsov, P. (2020). Combating the threats of cybercrimes in Russia evolution of the cybercrime laws and social concern. *Communist and Post-Communist Studies*, *53*(3), 123–136. https://doi.org/10.1525/cpcs.2020.53.3.123

Elin, V. M. (2022). On Approaches in Criminological Description of Persons Committing Crimes in the Computerized Information Sphere. *Rossiyskiy Sledovatel*, *7*, 61–65. (In Russ.). https://doi.org/10.18572/1812-3783-2022-7-61-65

Elin, V. M., & Zharova, A. K. (2009). On the allocation of data objects in a separate category of the crime object. *Proceedings of the Institute of State and Law, the Russian Academy of Sciences*, *5*, 205–229. (In Russ.).

Evdokimov, K. N. (2025). On improving the qualification of crimes in the field of computer information (based on judicial practice). *Rossiyskiy Sudya*, *2*, 36–40. (In Russ.). https://doi.org/10.18572/1812-3791-2025-2-36-40

Kurushin, V. D., & Minaev, V. A. (1998). *Computer crimes and informational security*. Moscow: New Lawyer. (In Russ.).

Onwuadiamu, G. (2025). Cybercrime in criminology; A systematic review of criminological theories, methods, and concepts. *Journal of Economic Criminology*, *8*(100136), 1–10. https://doi.org/10.1016/j.jeconc.2025.100136

Rossinskaya, E. R. (2021). The concept of the doctrine on information-computer forensic models as the basis of computer crime investigation techniques. *Vestnik Eastern Siberia Institute of the Ministry of the Interior of the Russian Federation*, *2*, 190–200. (In Russ.). https://doi.org/10.24412/2312-3184-2021-2-190-200

Russkevich, E. A. (2025). On conjunction of crimes in the sphere of computer information with other crimes. *Ugolovnoye Pravo*, *4*, 76–84. (In Russ.). https://doi.org/10.52390/20715870_2025_4_76

Sarkar, G., & Shukla, S. K. (2023). Behavioral analysis of cybercrime: Paving the way for effective policing strategies. *Journal of Economic Criminology*, *2*(100034), 1–26. https://doi.org/10.1016/j.jeconc.2023.100034

Shukan, A., Abdizhami, A., Ospanova, G., & Abdakimova D. (2019). Crime control in the sphere of information technologies in the Republic of Turkey. *Digital Investigation*, 30, 94–100. https://doi.org/10.1016/j.diin.2019.07.005

Unukovich, A. S. (2021). The concept of crimes committed with the use of information and telecommunication technologies. *Gosudarstvennaya Sluzhba i Kadry*, *4*, 278–280. (In Russ.). https://doi.org/10.24411/2312-0444-2021-4-278-280

Yazov, Yu. K. (2025). Cybersecurity terms and definitions. *Voprosy Kiberbezopasnosti*, *65*(1), 2–6. (In Russ.). https://doi.org/10.21681/2311-3456-2025-1-2-6

Younies, H., & Al-Tawil, T. N. (2020). Effect of cybercrime laws on protecting citizens and businesses in the United Arab Emirates (UAE). *Journal of Financial Crime*, *27*(4), 1089–1105. https://doi.org/10.1108/JFC-04-2020-0055

Zharova, A. K. (2019). Routing and IP to Ensure the Legal Regulation of Internet Relations. *RGGU Bulletin: Information Science. Information Security. Mathematics*, *2*, 32–42. (In Russ.). https://doi.org/10.28995/2686-679X-2019-2-32-42

Zharova, A. K. (2023a). Achieving Algorithmic Transparency and Managing Risks of Data Security when Making Decisions without Human Interference: Legal Approaches. *Journal of Digital Technologies and Law*, *4*, 973–993. (In Russ.). https://doi.org/10.21202/jdtl.2023.42

Zharova, A. K. (2023b). Artificial intelligence – a means of method committing fraud in the field of computer information? *State and Law*, *2*, 54–61. (In Russ.). https://doi.org/10.31857/S102694520021177-5

Zhmurov, D. V. (2024). The crime rate in the information and telecommunications technologies in 2019 to 2023 (the victimological aspect). *Rossiyskiy sudya*, *5*, 19–23. (In Russ.). https://doi.org/10.18572/1812-3791-2024-5-19-23

Вклад авторов

А. К. Жарова – методическое руководство исследованием, постановка цели и задач исследования, работа с научной литературой, работа с текстом статьи, изложение результатов и выводов.

Е. С. Анисимов – концепция статьи, работа с научной литературой, сбор и обработка данных, визуализация статистики, написание текста, обсуждение результатов, оформление статьи.

Author's contribution

A. K. Zharova – methodological guidance of research, setting research goals and objectives, working with scientific literature, working with the article text, presentation of results and conclusions.

E. S. Anisimov – article concept, working with scientific literature, data collection and processing, visualization of statistics, writing the text, discussion of results, formatting the article.

Информация об использовании искусственного интеллекта

ИИ не использовался.

Information about the use of artificial intelligence

AI was not used.

Конфликт интересов / Conflict of Interest

Авторами не заявлен / No conflict of interest is declared by the authors

История статьи / Article history

Дата поступления / Received 09.12.2025
Дата одобрения после рецензирования / Date of approval after reviewing 10.02.2026
Дата принятия в печать / Accepted 25.02.2026