Некоторые проблемы возбуждения уголовных дел о преступлениях в сфере информационно-телекоммуникационных технологий

Заливин Александр Николаевич
кандидат юридических наук, доцент, доцент кафедры уголовного процесса Московского университета МВД России имени В.Я. Кикотя, aleks-zalivin@mail.ru

В исследовании проблематизируется сложившаяся в 2024-2025 годах диспропорция между качественной трансформацией киберпреступности и инерционностью отечественного уголовно-процессуального механизма. Актуальность обсуждаемой темы продиктована парадоксальной статистической тенденцией последних лет: на фоне снижения валового количества регистрируемых IT-преступлений фиксируется рекордный рост материального ущерба и уровня латентности деяний. Целью в рамках статьи является выявление процессуальных дефектов стадии возбуждения уголовного дела, которые препятствуют эффективной фиксации «цифровых следов» и своевременной квалификации. В центре внимания автора находится явное противоречие между экстерриториальной, мгновенной природой сетевых хищений и архаичной, жестко регламентированной процедурой доследственной проверки, привязанной к физической географии вкупе с длительным бюрократическим согласованиям. На основе анализа научной литературы и статистических данных МВД РФ и Генпрокуратуры РФ резюмировано, что ключевым барьером служит не отсутствие уголовно-правовых запретов, а трудность оперативного получения сведений от провайдеров и банков в рамках сроков ст. 144 УПК РФ. Авторский вклад состоит в обосновании тезиса о том, что существующая практика «отказных» материалов является следствием системного конфликта между «тайной связи» и потребностями доказывания, который невозможно разрешить без внедрения упрощенных цифровых протоколов взаимодействия правоохранителей с финансовым сектором. Представленные материалы адресованы законодателям, специалистам в области уголовного процесса, судьям, сотрудникам следственных органов, ищущим пути оптимизации правоприменения в digital-среде.

Ключевые слова: возбуждение уголовного дела, квалификация преступлений, киберпреступность, компьютерная информация, мошенничество, подследственность, статистика преступности, территориальная юрисдикция, цифровые следы, электронные доказательства

Введение

Современная экономическая реальность характеризуется фундаментальными преобразованиями под воздействием цифровизации. Информационно-телекоммуникационные технологии (ИТТ) перестали быть обычным инструментом обеспечения бизнес-процессов. Они перешли в разряд самостоятельной среды существования капитала, прав собственности, деловых отношений. Как представляется, это формирует новые возможности для экономического роста. Вместе с тем, возникают и беспрецедентные угрозы. Криминализация цифрового пространства стала одним из ключевых вызовов для правоохранительной системы Российской Федерации в 2020-2025 годах.

Значимость обращения к теме исследования определяется существенным ростом киберпреступности, который, по сути, меняет криминальную статистику. Если в 2013 году количество преступлений, совершаемых с использованием ИТТ, исчислялось десятками тысяч, то к 2024 году данный показатель достиг 765 тысяч. Это составляет около 40% от общего массива регистрируемой преступности [3].

Между тем, статистика – лишь «верхушка айсберга». Ключевая проблема кроется в процессуальной плоскости, а именно – в стадии возбуждения уголовного дела. Именно на этом этапе правоприменитель сталкивается с коллизией между архаичными формами доследственной проверки и высокотехнологичной природой следообразования в сети. Сложность фиксации «цифровых следов», трансграничность преступлений, задействование злоумышленниками средств анонимизации (VPN, прокси-серверы, криптовалютные миксеры и т. д.) создают ситуацию, при которой значительная часть деяний остается либо латентной, либо «зависает» на этапе проверки сообщения о преступлении (из-за невозможности установить признаки состава в отведенные процессуальные сроки).

Помимо этого, экономический ущерб от подобных деяний растет несоразмерно их количеству. По данным МВД России, только за первые семь месяцев 2025 года ущерб от ИТ-преступлений увеличился на 16%; он составил почти 120 млрд рублей [2]. Это указывает на качественные изменения преступности: она становится профессиональнее, организованнее, технически изощреннее. В описываемом контексте анализ проблем возбуждения уголовных дел анализируемой категории приобретает как правовое, так и макроэкономическое значение, поскольку эффективность уголовного преследования напрямую влияет на инвестиционную привлекательность отечественной цифровой экономики.

Материалы и методы

В изученных при написании статьи источниках демонстрируется сочетание статистико-аналитического, уголовно-правового, криминалистического подходов к исследованию проблем возбуждения уголовных дел о преступлениях в сфере информационно-телекоммуникационных технологий. Этим обосновывается их комплексное использование в рамках заявленной темы.

Информационные и официально-статистические материалы [1-4, 8] опираются, главным образом, на эмпи-

рико-описательный и количественный анализ. В них фиксируется противоречивая динамика IT-преступности (рост ущерба и нераскрытых деяний при одновременном снижении общего числа преступлений). Это указывает на латентность и сложности первоначального этапа уголовного преследования.

В научных публикациях О.И. Захаренко, О.В. Ивушкиной, Т.Ф. Алиева, А.С. Сокольцовой, А.А. Лебедевой, Р.А. Рамазанова [5-7, 11] применяются уголовно-правовой, криминалистический, прикладной процессуальный подходы; авторы акцентируют внимание на типичных следственных ситуациях, алгоритмах возбуждения дел, профилактических механизмах. При этом по-разному оценивается достаточность действующих процедур и роль оперативно-розыскных мероприятий.

Анализ правового регулирования, представленный Е.Ю. Перевозниковой [9], базируется на формально-юридическом и системном методах. Выявляется фрагментарность нормативной базы. А разъяснения Пленума Верховного Суда РФ [10] отражают судебно-интерпретационный подход, который ориентирован на унификацию практики, но не учитывается в полной мере специфика цифровых способов совершения преступлений.

Пробелы литературы проявляются в недостаточной проработке критериев повода и основания для возбуждения уголовного дела именно в цифровой среде, а противоречия – в расхождении статистических оценок и в различной трактовке приоритета процессуальной экономии и защиты прав потерпевших. В связи с этим при подготовке статьи использованы следующие методы: формально-юридический, системный, статистический; проведен анализ судебной и следственной практики; задействованы элементы криминалистического моделирования. Это позволяет согласовать нормативные предписания с реальными условиями возбуждения и начального этапа расследования IT-преступлений.

Результаты и обсуждение

Для понимания масштаба рассматриваемой в статье проблемы требуется обратиться к цифрам. Анализ данных ГИАЦ МВД России и Генеральной прокуратуры позволяет выявить интересную тенденцию: после многолетнего непрерывного роста в 2025 году наметилась некоторая стабилизация количественных показателей, сопровождающаяся, однако, ростом тяжести последствий [4, 8]. В таблице 1 представлены ключевые сведения о состоянии киберпреступности за последние два отчетных периода.

Таблица 1

Динамика преступлений, совершенных с использованием ИТТ в РФ (сравнительный анализ 2024-2025 гг.) (составлено на основе [2-4, 8])

Показатель	2024 год (итоговые значения)	Январь-ноябрь 2025 года	Динамика (2025 к 2024, %)
Общее количество зарегистрированных преступлений ИТТ	765 000	627 000	Снижение на 10,8% (в годовом выражении к аналог. периоду)
Удельный вес ИТТ в общей структуре преступности	40,0%	38,2%	Снижение на 1,8 п.п.
Материальный ущерб (млрд руб.)	~100,5 (за 7 мес. 2024 г.)	119,6 (за 7 мес. 2025 г.)	Рост на 16%
Количество нераскрытых преступных деяний	Рост на 20% к 2023 г.	Данные уточняются	Тенденция к росту латентности
Доля мошенничеств и краж (в структуре ИТТ)	~65%	62,5%	Стабильно высокая доля

Анализируя информацию из таблицы 1, уместно предположить, что снижение общего вала регистрации в 2025 году сопряжено не столько с реальным уменьшением криминальной активности, сколько с эффектом «высокой базы» предыдущих лет и, вероятно, с изменением методики учета либо усложнением процедур возбуждения дел по неочевидным составам. Примечателен рост материального ущерба на фоне снижения количества эпизодов. Это прямо указывает на укрупнение среднего размера хищения. Киберпреступники переходят от массовых атак с низким чеком к таргетированным ударам по корпоративному сектору и состоятельным гражданам.

Особую тревогу вызывает статистика раскрываемости. В 2024 году число нераскрытых ИТ-преступлений выросло на 20%. Это говорит о системном отставании оперативных служб от технического прогресса криминалитета. По существу, три четверти киберпреступлений остаются безнаказанными. В итоге подпитывается чувство безнаказанности и провоцируются рецидивы. В структуре деяний превалируют хищения (кражи и мошенничества) – более 62%. При этом наблюдается тревожный рост наркопреступлений, которые совершаются бесконтактным способом (+51,6% в структуре ИТТ) [1].

Стадия возбуждения уголовного дела (ст. 140-148 УПК РФ) является фильтром, который помогает отсеивать гражданско-правовые споры от криминала, но в то же время обеспечивать быстрое реагирование. В сфере ИТТ он функционирует с перебоями.

Во-первых, серьезной проблемой становится установление места совершения преступления (для определения территориальной подследственности). В отличие от физического мира, где оно локализовано, в киберпространстве хищение может начаться в одном регионе (место нахождения злоумышленника), проходить через серверы в другом, а ущерб наступать в третьем (локация открытия счета потерпевшего). Пленум Верховного Суда РФ неоднократно давал разъяснения по данному вопросу, закрепляя место совершения, например, для безналичных хищений, как локацию нахождения банка потерпевшего или совершения действий лицом. Однако на практике материалы проверки часто «гуляют» между регионами, пересылаемые по территориальности, пока истекают сроки хранения цифровых следов у провайдеров [5, 7, 11].

Во-вторых, существуют явные трудности квалификации деяния на этапе проверки сообщения. Следователю необходимо в сжатые сроки (3, 10, максимум 30 суток) определить, имеет ли место состав ст. 159.6 УК РФ («Мошенничество в сфере компьютерной информации») или «обычное» мошенничество (ст. 159 УК РФ), но с применением электронных средств. Разграничение, как показывает судебная практика, неочевидно [9, 10].

В Таблице 2 приведено сравнение подходов к квалификации, которое базируется на анализе судебных решений и разъяснений Пленума ВС РФ № 48 (Постановление от 30.11.2017 № 48, ред. от 15.12.2022).

Таблица 2

Разграничение составов преступлений при возбуждении уголовных дел (составлено на основе [6, 10])

Критерий	Ст. 159.6 УК РФ (компьютерное мошенничество)	Ст. 159 УК РФ (в т.ч. с использованием ИТТ)
Способ хищения	Ввод, удаление, блокирование, модификация компьютерной информации. Вмешательство в работу алгоритмов и систем	Обман или злоупотребление доверием *человека*. Компьютер используется лишь как средство связи
Объект воздействия	Техническое устройство, сервер, база данных, программный код	Сознание и воля потерпевшего (или сотрудника организации)
Пример из практики	Взлом банковского приложения, изменение баланса счета путем SQL-инъекции	Звонок от «службы безопасности банка», убеждение жертвы самостоятельно перевести средства
Проблемы при возбуждении	Требует технической экспертизы или участия специалиста на этапе проверки для подтверждения факта вмешательства	Требует установления факта обмана, фиксации переписки, аудиозаписей

Сложность проявляется в том, что на этапе доследственной проверки у дознавателя или следователя зачастую нет технической возможности установить, было ли вмешательство в систему (ст. 159.6) либо просто использование чужих учетных данных (что чаще квалифицируется как кража с банковского счета – п. «г» ч. 3 ст. 158 УК РФ). Неверная квалификация на старте влечет за собой проведение не тех следственных действий, утрату доказательств и, как результат, возвращение дел прокурором или судом.

В-третьих, специфической проблемой является сбор доказательственной базы до возбуждения дела. Для получения сведений о соединениях (биллинг), IP-адресах, движениях по счетам требуется судебное решение (если речь идет о тайне связи / банковской тайне) или длительные запросы. В рамках сроков ст. 144 УПК РФ получить ответы от банковских организаций и провайдеров (особенно зарубежных) практически невозможно. Это вынуждает правоохранителей либо выносить «отказные» постановления с целью их последующей отмены и проведения дополнительной проверки (создавая «карусель» проверок), либо возбуждать дело по факту («глухарь»), заведомо понимая низкую перспективу его раскрытия.

Заключение

Механизм возбуждения уголовных дел о преступлениях в сфере ИТТ в Российской Федерации, невзирая на наработанную практику, требует системной донастройки. Посредством статистики последних лет демонстрируется противоречивая картина: количественное снижение регистрации на фоне роста ущерба, латентности. Это сигнализирует о том, что существующая процессуальная форма не успевает за эволюцией криминальных технологий.

По-видимому, ключевым направлением усовершенствования должно стать не столько ужесточение санкций (они в ст. 159.6 УК РФ и так предусматривают до 10 лет лишения свободы), сколько оптимизация процедуры доследственной проверки. Представляется целесообразным рассмотреть возможность внедрения упрощенного порядка получения сведений об электронных соединениях и транзакциях на этапе проверки сообщения о преступлении, возможно, через создание единой защищенной платформы взаимодействия между МВД РФ, ЦБ РФ, операторами связи.

В дополнение к отмеченному, назрела необходимость в повышении уровня цифровой грамотности сотрудников органов предварительного расследования. Ошибки в квалификации (путаница между ст. 159, 158, 159.6 УК РФ) нередко проистекают из непонимания технической сути деяния. В этой связи, вероятно, уместно расширить практику привлечения специалистов в области компьютерной информации уже на стадии приема заявления о преступлении. Без этих мер противодействие киберпреступности рискует остаться борьбой с последствиями, а не с причинами. В это недопустимо в условиях, когда цифровая экономика становится основой суверенитета страны.

Литература

1. В России выросло число нераскрытых IT-преступлений // URL: https://infoforum.ru/smi-o-nas/v-rossii-vyroslo-chislo-neraskrytyh-it-prestuplenij (дата обращения: 26.01.2026).

2. В России за январь–июль 2025 года ущерб от IT-преступлений вырос на 16% и составил почти 120 млрд рублей // URL: https://alrf.ru/news/v-rossii-za-yanvar-iyul-2025-goda-ushcherb-ot-it-prestupleniy-vyros-na-16-i-sostavil-pochti-120-mlrd/ (дата обращения: 26.01.2026).

3. Генпрокуратура России: IT-преступления снизились на 10,8% в 2025 // URL: https://tsargrad.tv/novost/genprokuratura-rossii-prestuplenija-snizilis-na-108-v-2025_1506090 (дата обращения: 26.01.2026).

4. Динамика преступлений в сфере информационных технологий: статистика МВД 2022-2025 гг. // URL: https://promrating.ru/news/dinamika-prestuplenij-v-sfere-informaczionnyh-tehnologij-statistika-mvd-2022-2025-gg/ (дата обращения: 26.01.2026).

5. Захаренко О.И. Возможности повышения эффективности борьбы с преступлениями, совершаемыми в сфере информационно-телекоммуникационных технологий // Законность. – 2024. – № 9 (1079). – С. 56-58.

6. Ивушкина О.В., Алиев Т.Ф., Сокольцова А.С. Особенности предупреждения преступления, предусмотренного ст. 159.6 УК РФ // Научный дайджест Восточно-Сибирского института МВД России. – 2024. – № 4 (26). – С. 37-43.

7. Лебедева А.А. Исходные следственные ситуации и рекомендуемые алгоритмы расследования киберпреступлений // Расследование преступлений: проблемы и пути их решения. – 2021. – № 4 (34). – С. 64-70.

8. МВД России публикует статистическую информацию о состоянии преступности в Российской Федерации за январь-ноябрь 2025 года // URL: https://mvdmedia.ru/news/official/informatsiya-o-sostoyanii-prestupnosti-v-rossiyskoy-federatsii-za-yanvar-noyabr-2025-goda/ (дата обращения: 26.01.2026).

9. Перевозникова Е.Ю. Современное состояние правового регулирования преступлений в сфере информационно-телекоммуникационных технологий // Технологии XXI века в юриспруденции. Материалы Шестой всероссийской научно-практической конференции. – Екатеринбург: 2024. – С. 102-108.

10. Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 (ред. от 15.12.2022) «О судебной практике по делам о мошенничестве, присвоении и растрате» // URL: https://www.consultant.ru/document/cons_doc_LAW_283918/ (дата обращения: 26.01.2026).

11. Рамазанов Р.А. Особенности возбуждения уголовного дела и первоначального этапа расследования преступлений в сфере информационно-телекоммуникационных технологий // Журнал правовых и экономических исследований. – 2022. – № 3. – С. 161-167.

Some issues of initiating criminal cases on crimes in the field of information and telecommunications technologies

Zalivin A.N.

Kikot Moscow University of the Ministry of Internal Affairs of Russia

The study problematizes the imbalance that emerged in 2024–2025 between the qualitative transformation of cybercrime and the inertia of the domestic criminal procedure framework. The relevance of the topic is driven by a paradoxical statistical trend of recent years: against the backdrop of a decline in the total number of registered IT-related crimes, a record increase in material damage and the level of latency has been observed. The purpose of the article is to identify procedural defects at the stage of initiating criminal proceedings that hinder the effective preservation of “digital traces” and the timely legal qualification of offenses. The author focuses on the evident contradiction between the extraterritorial and instantaneous nature of online theft and the archaic, rigidly regulated pre-investigation procedure, which remains tied to physical geography and prolonged bureaucratic approvals. Based on an analysis of academic literature and statistical data from the Ministry of Internal Affairs of the Russian Federation and the Prosecutor General's Office of the Russian Federation, it is concluded that the key barrier is not the absence of criminal law prohibitions, but the difficulty of promptly obtaining information from service providers and banks within the time limits established by Article 144 of the Criminal Procedure Code of the Russian Federation. The author’s contribution lies in substantiating the thesis that the prevailing practice of issuing refusals to initiate criminal proceedings results from a systemic conflict between the secrecy of communications and the needs of criminal proof, a conflict that cannot be resolved without introducing simplified digital protocols for interaction between law enforcement agencies and the financial sector. The materials are addressed to legislators, scholars in criminal procedure, judges, and investigative practitioners seeking ways to optimize law enforcement in the digital environment.

Keywords: initiation of criminal proceedings, crime qualification, cybercrime, computer information, fraud, investigative jurisdiction, crime statistics, territorial jurisdiction, digital traces, electronic evidence

References

1. The number of unsolved IT crimes has increased in Russia // URL: https://infoforum.ru/smi-o-nas/v-rossii-vyroslo-chislo-neraskrytyh-it-prestuplenij (date of access: 01/26/2026).
2. In Russia, in January–July 2025, the damage from IT crimes increased by 16% and amounted to almost 120 billion rubles // URL: https://alrf.ru/news/v-rossii-za-yanvar-iyul-2025-goda-ushcherb-ot-it-prestupleniy-vyros-na-16-i-sostavil-pochti-120-mlrd/ (date of access: 01/26/2026).
3. Russian Prosecutor General's Office: IT crimes decreased by 10.8% in 2025 // URL: https://tsargrad.tv/novost/genprokuratura-rossii-prestuplenija-snizilis-na-108-v-2025_1506090 (date of access: 01/26/2026).
4. Dynamics of crimes in the field of information technology: statistics of the Ministry of Internal Affairs 2022-2025 // URL: https://promrating.ru/news/dinamika-prestuplenij-v-sfere-informaczionnyh-tehnologij-statistika-mvd-2022-2025-gg/ (date of access: 01/26/2026).
5. Zakharenko O.I. Possibilities of increasing the effectiveness of combating crimes committed in the field of information and telecommunication technologies // Legality. – 2024. – No. 9 (1079). – Pp. 56-58.
6. Ivushkina O.V., Aliev T.F., Sokoltsova A.S. Features of crime prevention under art. 159.6 of the Criminal Code of the Russian Federation // Scientific digest of the East Siberian Institute of the Ministry of Internal Affairs of Russia. – 2024. – No. 4 (26). – Pp. 37-43.
7. Lebedeva A.A. Initial investigative situations and recommended algorithms for investigating cybercrimes // Crime investigation: problems and solutions. – 2021. – No. 4 (34). – Pp. 64-70.
8. The Ministry of Internal Affairs of Russia publishes statistical information on the state of crime in the Russian Federation for January-November 2025 // URL: https://mvdmedia.ru/news/official/informatsiya-o-sostoyanii-prestupnosti-v-rossiyskoy-federatsii-za-yanvar-noyabr-2025-goda/ (date of access: 01/26/2026).
9. Perevoznikova E.Y. The current state of legal regulation of crimes in the field of information and telecommunication technologies // Technologies of the XXI century in jurisprudence. Materials of the Sixth All-Russian Scientific and Practical Conference. – Yekaterinburg: 2024. – Pp. 102-108.
10. Resolution of the Plenum of the Supreme Court of the Russian Federation dated 11/30/2017 No. 48 (as amended on 12/15/2022) "On judicial practice in cases of fraud, embezzlement and embezzlement" // URL: https://www.consultant.ru/document/cons_doc_LAW_283918/ (date of access: 01/26/2026).
11. Ramazanov R.A. Features of the initiation of a criminal case and the initial stage of the investigation of crimes in the field of information and telecommunication technologies // Journal of Legal and Economic Research. – 2022. – No. 3. – Pp. 161-167.