Дата поступления рукописи в редакцию: 04.10.2026 г. DOI: 10.24412/2224-9133-2026-10-401-406
Дата принятия рукописи в печать: 10.11.2026 г.

КУЗНЕЦОВ Роман Александрович,
аспирант 3 курс Российская Таможенная Академия, Российская таможенная, г. Люберцы,
e-mail: romank2004@inhox.ru

ОСОБЕННОСТИ ДОСУДЕБНОГО ПРОИЗВОДСТВА ПО ДЕЛАМ О ТАМОЖЕННЫХ КИБЕРПРЕСТУПЛЕНИЯХ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация. *В настоящей научной статье автор кратко рассматривает особенности досудебного производства по делам о таможенных киберпреступлениях в РФ. Автор исследования отмечает высокий уровень распространения киберпреступности в целом, анализирует статистические материалы. Далее автор статьи также акцентирует внимание уже на конкретных проблемах, с которыми сталкиваются органы следствия и дознания при осуществлении досудебного производства по делам о таможенных киберпреступлениях. В научной работе сделан акцент на необходимость совершенствования действующего правового регулирования, правоприменительной практики, а также методической составляющей данного процесса. Объектом исследования являются особенности досудебного производства по делам о таможенных киберпреступлениях в РФ. Целью исследования является комплексный, последовательный анализ особенностей досудебного производства по делам о таможенных киберпреступлениях в РФ. Методы исследования: формально-юридический, компаративистский, сравнительный анализ, диалектический, обобщение, конкретизация, систематизация и системный метод, дедукция, иные методы теоретического и практического уровней научного познания. Научная новизна исследования заключается в подготовке комплексного исследования, формировании авторских выводов относительно особенностей досудебного производства по делам о таможенных киберпреступлениях в РФ. Данная научная статья, таким образом, будет полезна теоретикам, практикам, обучающимся и профессорско-преподавательскому составу гуманитарных и иных направлений подготовки, а также более широкому кругу читателей, интересующихся особенностями досудебного производства по делам о киберпреступлениях и таможенных киберпреступлениях в РФ в частности в современном российском уголовно-процессуальном праве.*

Ключевые слова: *досудебное производство, уголовный закон, киберпреступность, киберпреступление, уголовный процесс, современное состояние.*

Для цитирования: *Кузнецов Р. А. Особенности досудебного производства по делам о таможенных киберпреступлениях в Российской Федерации // Право и управление. 2026. № 10. С. 401–406.*

KUZNETSOV Roman Alexandrovich,
PhD student, 3rd year, Russian Customs Academy, Russian Customs, Lyubertsy

FEATURES OF PRE-TRIAL PROCEEDINGS IN CASES OF CUSTOMS CYBERCRIME IN THE RUSSIAN FEDERATION

Annotation. *In this scientific article, the author briefly examines the features of pre-trial proceedings in cases of customs cybercrime in the Russian Federation. The author of the study notes the high level of cybercrime prevalence in general, analyzes statistical materials. Further, the author of the article also focuses on the specific problems faced by the investigative and inquiry bodies in the implementation of pre-trial proceedings in cases of customs cybercrime. The scientific work focuses on the need to improve the current legal regulation, law enforcement practice, as well as the methodological component of this process. The object of the study is the peculiarities of pre-trial proceedings in cases of customs cybercrime in the Russian Federation. The aim of the study is a comprehensive, consistent analysis of the features of pre-trial*

proceedings in cases of customs cybercrime in the Russian Federation. Research methods: formal legal, comparative, comparative analysis, dialectical, generalization, concretization, systematization and system method, deduction, other methods of theoretical and practical levels of scientific knowledge. The scientific novelty of the study is the preparation of a comprehensive study, the formation of author's conclusions on the specifics of pre-trial proceedings in cases of customs cybercrime in the Russian Federation. This scientific article, therefore, will be useful for theorists, practitioners, students and teaching staff in the humanities and other fields of study, as well as for a wider range of readers interested in the specifics of pre-trial proceedings in cases of cybercrime and customs cybercrime in the Russian Federation, in particular in modern Russian criminal procedure law.

Key words: *pre-trial proceedings, criminal law, cybercrime, cybercrime, criminal process, current state.*

For citation: *Kuznetsov R. A. Features of pre-trial proceedings in cases of customs cybercrime in the Russian Federation. Law and administration. 2026;(10):401–406. (In Russ.).*

В современной отечественной уголовно-правовой практике киберпреступность приобрела крайне широкое распространение, и статистические показатели по совершению преступлений данной категории ежегодно продолжают расти. Причем, как отмечает МВД России, если количественные показатели по данным преступлениям показывают некоторый спад, качественные характеристики, напротив, становятся все значительнее [5]. Это касается, в первую очередь, размера нанесенного совершением киберпреступлений имущественного ущерба.

В частности, за первое полугодие 2026 г. общее число совершенных киберпреступлений сократилось на 30 % в сравнении с аналогичным периодом прошлого года – с 371,4 тыс случаев до 252,9 тыс. В свою очередь, нанесенный ущерб по итогам первого полугодия 2025 г. составил более 480 млн рублей, в то время как первое полугодие 2026 г. «закрылось» показателем в 1,4 млрд рублей, что в три раза больше, чем в минувшем году [6; 11]. Наибольший урон при этом несут такие отрасли экономики страны, как государственный сектор и промышленность, финансы и ИТ, а также транспорт (диаграмма 1) [4].

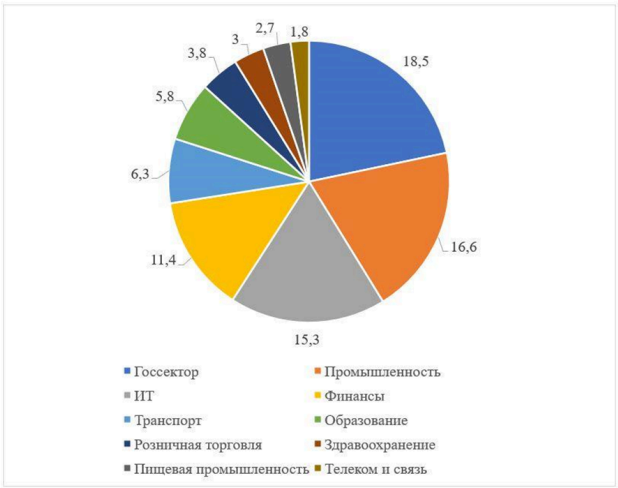


Диаграмма 1. Статистика распространения киберпреступлений в России за период 2023-2026 гг. (по материалам Обзора «Лаборатории Касперский», специально для ПМЭФ-2026 г.) [4].

Специалисты отмечают и ряд других актуальных характеристик киберпреступности, среди которых ключевой выступает качественная трансформация схем совершения преступлений, появление новых механизмов, при этом все больше на практике встречается «чистых» способов манипуляций, крайне сложных для проведения расследования и привлечения к ответственности. В конечном итоге, можно уверенно сделать вывод: сегодня киберпреступления занимают одну из главенствующих позиций в структуре преступлений против собственности, а его новые цифровые формы формируют самостоятельный массив уголовных дел [6; 11]. Полагаем, в дальнейшем данная трансформация продолжится, что сохранит высокую степень актуальности рассматриваемой темы исследования.

В сфере реализации таможенных правоотношений киберпреступления также составляют довольно существенный процент, ключевой причиной тому служит высокая степень цифровизации разного рода таможенных процессов. В частности, наиболее распространенными категориями выступают следующие виды:

совершение атак на государственные информационные системы: DDoS-атаки, внедрение вредоносного программного обеспечения, атаки на критическую информационную инфраструктуру;

совершение преступлений, связанных с информацией и данными: утечки и компрометация баз данных, незаконный сбор и хранение, распространение персональных данных (ст. 272.1 УК РФ);

совершение экономических преступлений с использованием цифровых каналов: уклонение от уплаты таможенных платежей с применением ИТ (ст. 194 УК РФ), контрабанда с применением ИТ (ст.ст. 200.1, 226.1, 229.1 УК РФ), совершение валютных операций по переводу денежных средств с применением для этого поддельной документации (ст. 193.3 УК РФ);

совершение преступлений против информационной инфраструктуры: создание и распространение вредоносных программ (ст. 273 УК РФ), нарушение правил эксплуатации информационных сетей (ст. 274 УК РФ);

социальная инженерия и совершение фишинговых атак, а также другое [1; 7].

Таким образом, как показывает анализ статистической информации, сегодня совершение киберпреступлений в таможенной сфере является актуальной проблемой. Специалисты обращают внимание на проблемный характер таких уголовных дел, ряд сложностей, возникающих и на досудебном, и на судебном этапах расследования. Далее более детально будет рассмотрена именно досудебная стадия производства.

Прежде всего, существенной проблемой на досудебном этапе выступает правильное определение подследственности и подсудности. Здесь необходимо отметить два важных момента. Во-первых, это высокий уровень трансграничности киберпреступлений. Благодаря развитию цифровых технологий лица, совершающие такие преступления, могут находиться не только за пределами территории России, но также и на территориях разных государств (к примеру, если преступление совершается организованной группой лиц). В подобной ситуации крайне сложным может являться и определение места совершения киберпреступления, и конкретного местоположения лиц, его совершивших, что существенно усложняет и процедуру возбуждения уголовного дела, его расследования, и впоследствии – привлечение виновных лиц к уголовной ответственности. Поэтому для киберпреступлений в большинстве случаев потенциально актуальной проблемой является фактическая невозможность привлечения к уголовной ответственности.

Формально основным ведомственным субъектом, в чьи функции входит выявление и осуществление первичной проверки фактов совершения киберпреступлений, является Федеральная таможенная служба России (далее – ФТС России) в лице структурных подразделений по борьбе с контрабандой и оперативно-розыскных подразделений. Тем не менее, по ряду составов, согласно нормам УПК РФ, предусматривается осуществление досудебного производства Следственным комитетом России или МВД России – например, это ст. 226.1 УК РФ. ФТС России в подобной ситуации все же принимает участие в проведении следственных действий, однако только в пределах реализации функций органа дознания [9].

Во-вторых, следует отметить также особенности, характеризующие поводы и основания для возбуждения уголовного дела по совершению таможенных киберпреступлений. Так, в привычном выражении состава контрабанды основанием выступает производство физического досмотра груза, т.е., совершение каких-либо реальных действий с материальными объектами. В области ИТ специфика существенно отличается. Здесь основанием для возбуждения уголовного дела могут выступать, к примеру, срабатывание систем управления рисками ФТС России, действующих в автоматическом режиме, получение от кредитных организаций сообщений о совершении подозрительных валютных операций, связанных с фиктивным импортом, получение при осуществлении мониторинговых действий в сети Интернет материалов оперативно-розыскной деятельности, и другое. Во многом процедура выявления и пресечения таможенных киберпреступлений усложняется тем, что рассматриваемые противоправные процессы происходят, как правило, внутри какой-либо внутренней информационной системы ФТС России либо в аналогичных комплексах, поэтому субъект выявления и пресечения здесь специальный – именно таможенные органы всецело несут ответственность за эффективность процесса [9]. Условно говоря, такое преступление не может быть обнаружено случайно сторонним лицом (как, к примеру, в случае с кражей лицо обнаружило открытую дверь в жилое помещение соседей, обратилось с подозрением в правоохранительные органы, и т.д.). С другой стороны, подобная профильность субъектов снижает общий уровень латентности киберпреступлений, совершаемых в таможенной сфере.

В-третьих, особенностью досудебного производства и серьезной практической проблемой в данном случае выступает процесс доказывания и сбор цифровых следов непосредственно. Сегодня вопрос легализации цифровых доказательств остается недостаточно четко урегулированным с правовой точки зрения, а постоянное развитие ИТ и, соответственно, возникновение качественно новых видов цифровых следов создает пробелы в правовом регулировании. К примеру, в судебной практике широко встречается фиксация сетевого трафика и логов – т.е., изъятие имеющихся данных о подключениях по IP и MAC-адресам, что позволяет качественно идентифицировать конкретное используемое устройство. Другими распространенными доказательствами в делах о таможенных киберпреступлениях выступают экспертные заключения (прежде всего, это компьютерно-технические и информационно-аналитические экспертизы, которые проводит профильное экспертно-криминалистическое управление, входящее в структуру ФТС России), а также разного рода облачные сервисы, чаще всего используемые при совершении противоправных действий на трансграничном уровне. Безусловно, если речь идет о расследовании трансграничных та-

моженных киберпреступлений (которых в общей статистике более 70 % от общего числа совершаемых таможенных киберпреступлений), то здесь ключевым направлением выступает взаимодействие с таможенными органами других государств по вопросу сбора и легализации доказательств. Правовым процессуальным инструментом в данном случае выступает международно-правовое поручение.

В-четвертых, характерной особенностью досудебного производства по делам о таможенных киберпреступлениях является сочетание производства таможенных проверок и следственных действий, предусмотренных нормами УПК РФ. К примеру, речь идет о проверке достоверности сведений о выпуске товаров, право на проведение которой таможенные органы имеют в течение трех лет после их выпуска. В цифровом смысле необходимым представляется исследование архивных данных электронных систем декларирования и других схожих комплексов.

Иным примером в данном случае может служить наложение ареста на электронные денежные средства – мера процессуального принуждения, нормативно установленная ст. 115 УПК РФ. В контексте совершения именно таможенных киберпреступлений речь идет о наложении ареста не только на непосредственно банковские счета, но также на разного рода электронные кошельки, криптовалютные активы, а также иные объекты, используемые для совершения киберпреступления [1].

Таким образом, как видно из перечисленного выше перечня, доступного к расширительному толкованию, в настоящее время осуществление досудебного производства по делам о таможенных киберпреступлениях обладает значительными особенностями, в т.ч. в сравнении с расследованием дел по другим видам киберпреступлений. Некоторые из них упрощают досудебное производство, другие – напротив, делают его более длительным, сложным, проблемным. Отметим несколько основных причин, способствующих такому выводу.

Прежде всего, проблемным выступает правовое регулирование. В целом, если рассматривать цифровизацию вне отраслевой зависимости, то очевидным будет вывод о том, что сегодня российское право «не успевает» за темпами развития ИТ. На это обращают внимание многие эксперты, акцентирующие внимание на том, что для качественного развития правового регулирования требуется «мощный триггер», и ключевой проблемой в данном случае выступает искусственный интеллект (далее – ИИ). И если в отношении совершенствования расследования киберпреступлений в целом законодателем был принят ряд значимых правовых документов (преимущественно декларативного характера – к примеру, это Государственная программа «Информационное общество», утвержденная Постановлением Правительства РФ от 15.04.2014 г. № 313, Стратегия действий в интересах граждан старшего поколения в РФ, утвержденная Распоряжением Правительства РФ от 07.04.2025 г. № 830-р, и другие), то именно в части расследования таможенных киберпреступлений в настоящее время нет ни одного правового или неправового документа, кроме некоторых ведомственных актов. К слову, подобная проблема характерна не только для таможенных, но и для других разновидностей киберпреступлений. Иными словами, законодатель ожидаемо идет по дедуктивному пути от общего к частному, однако в настоящее время ни общее, ни профильное правовое регулирование спорного вопроса не предусмотрено. Проблемным с точки зрения внедрения цифровых элементов выступает и непосредственно УПК РФ, однако этот вопрос постепенно решается, хотя и здесь темпы актуализации правового регулирования ожидаемо «не успевают» за развитием ИТ.

Аналогичным образом можно охарактеризовать и правоприменительную практику по делам о таможенных киберпреступлениях. В настоящее время нет ни одного разъясняющего документа от ВС РФ, где бы намечался вектор осуществления досудебного и судебного производства по делам данной категории, что вызывает сложности при расследовании, а на судебной стадии – мешает качественному формированию единообразной судебной практики. Это касается, к примеру, процедуры оценки доказательств судом.

Тем не менее, наиболее существенной в рассматриваемом контексте все же выступает проблема методического обеспечения. Здесь ситуация развивается аналогично правовому регулированию – методическая база в идеальном варианте должна совершенствоваться и обновляться сообразно развитию ИТ, однако на практике это происходит существенно медленнее. Усложняет процедуру кадровый вопрос, поскольку качественное расследование таможенных киберпреступлений возможно только в ситуации, когда высоким уровнем компьютерной грамотности обладают не только сотрудники правоохранительных, но и таможенных органов. Общеизвестной является проблема нехватки квалифицированных технических специалистов, профильных криминалистов, что увеличивает сроки расследования киберпреступлений и усложняет сам процесс. В контексте технико-криминалистической составляющей экспертами также отмечается и ряд иных значимых проблем:

высокий уровень анонимизации лиц, совершающих противоправные деяния;

активное развитие и использование при со-

вершении киберпреступлений ИИ;

сложность работы с цифровыми доказательствами;

иное.

Дополнительно в качестве проблемных направлений в рассматриваемом контексте зачастую выделяют вопросы межведомственного взаимодействия, сложный характер коммуникации с частным сектором предпринимательства, и ряд других.

Кратко обобщим изложенное, сделаем выводы.

Предметом исследования в научной статье стали особенности досудебного производства по делам о таможенных киберпреступлениях в РФ.

Прежде всего, автором была проанализирована статистическая информация, что позволило сделать вывод о количественном снижении общего уровня киберпреступности, но о его качественном росте [6; 11]. Существенно вырос размер максимального имущественного ущерба, наносимого преступлениями данной категории. К сожалению, в настоящее время нельзя говорить о наличии тенденции к позитивным изменениям.

Таможенные киберпреступления обладают своими характерными особенностями, что, соответственно, оказывает влияние и на досудебное производство по таким делам. В частности, в научной статье выделяются следующие отличительные черты:

необходимость правильного определения подследственности и подсудности;

высокий уровень трансграничности киберпреступлений;

специфические поводы и основания для возбуждения уголовного дела;

более сложный и продолжительный процесс доказывания и сбор цифровых следов;

сочетание производства таможенных проверок и следственных действий, предусмотренных нормами УПК РФ; иное [1; 9].

В конечном итоге, автор акцентирует внимание на трех глобальных проблемных составляющих досудебного производства по делам о таможенных киберпреступлениях: это правовое регулирование, правоприменительная практика и методическая, технико-криминалистическая часть. Особого внимания заслуживают первая и последняя, поскольку в значительной степени именно от их эффективности зависит качество проведения расследования по делам данной категории. К сожалению, в настоящее время нельзя прогнозировать существенные позитивные изменения, хотя определенные попытки совершенствования, как видно из представленных в научной статье примеров, и законодатель, и правоприменитель все же делают.

Полагаем, рассматриваемая тема останется крайне актуальной и в дальнейшем.

Список литературы:

[1] Гриненко, А.В. Уголовно-процессуальный кодекс РФ: постатейный научно-практический комментарий: учебное пособие. – 5-е изд., перераб. и доп. – М.: Проспект, 2026. – 1104 с.

[2] Ищенко, П.П. Современные подходы к цифровизации досудебного производства по уголовным делам // Lex russica. – 2019. – № 12. – С. 68-79.

[3] Кузнецов, Р.А. Понятие и общественная опасность киберпреступления в таможенной сфере // Международный научный вестник. – 2024. – № 11. – С. 15-22.

[4] Обзор 2026: Лаборатория Касперский – о киберугрозах современной России (специально для ПМЭФ-2026) [Электронный ресурс] – Режим доступа: – URL: https://content.kaspersky-labs.com/se/media/ru/business-security/enterprise/cyberpulse-general-2025.pdf.

[5] Официальный сайт МВД России [Электронный ресурс] – Режим доступа: – URL: https://мвд.рф/.

[6] Методические рекомендации по осуществлению прокурорского надзора за исполнением законом при расследовании преступлений в сфере компьютерной информации (утв. Генпрокуратурой России 15.04.2014 г.). Документ опубликован не был. Доступ из СПС «КонсультантПлюс».

[7] Мошенничество и киберпреступность в 2025 – начале 2026 г.: статистика [Электронный ресурс] – Режим доступа: – URL: https://alrf.ru/articles/moshennichestvo-i-kiberprestupnost-v-2025-nachale-2026-goda/.

[8] Постановление Пленума Верховного Суда РФ от 15.12.2022 г. № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть "Интернет"». Российская газета. 2022. № 294.

[9] Федеральная таможенная служба: Таможенные органы возбудили свыше 660 уголовных дел в 1 квартале 2025 года [Электронный ресурс] – Режим доступа: – URL: https://customs.gov.ru/press/federal/document/633037.

[10] Хроменков, И.Р., Качалова О.В. Обеспечение судом правовых интересов в досудебных стадиях российского уголовного судопроизводства: монография. – М.: Проспект, 2023. – 176 с.

[11] Число киберпреступлений в РФ за полгода 2026 г. сократилось на 30 % [Электронный ресурс] – Режим доступа: – URL: https://www.kommersant.ru/doc/8816431.

References:

[1] Grinenko, A.V. Code of Criminal Procedure of the Russian Federation: article-by-article scientific and practical commentary: textbook. - 5th ed., Revised and add. - M.: Prospect, 2026. - 1104 s.

[2] Ishchenko, P.P. Modern approaches to digitalization of pre-trial criminal proceedings // Lex russica. – 2019. – № 12. - S. 68-79.

[3] Kuznetsov, R.A. The concept and public danger of cybercrime in the customs sphere // International Scientific Bulletin. – 2024. – № 11. - S. 15-22.

[4] Review 2026: Kaspersky Lab - about the cyber threats of modern Russia (specially for SPIEF-2026) [Electronic resource] - Access mode: - URL: https://content.kaspersky-labs.com/se/media/ru/business-security/enterprise/cyberpulse-general-2025.pdf.

[5] Official website of the Ministry of Internal Affairs of Russia [Electronic resource] - Access mode: - URL: https://мвд.рф/.

[6] Guidelines for the implementation of prosecutorial supervision of the implementation of the law in the investigation of crimes in the field of computer information (approved by Prosecutor General of Russia 15.04.2014 g.). The document was not published. Access from SPS "ConsultantPlus.".

[7] Fraud and cybercrime 2025 - early 2026: Statistics [Electronic Resource] - Access Mode: - URL: https://alrf.ru/articles/moshennichestvo-i-kiberprestupnost-v-2025-nachale-2026-goda/.

[8] Resolution of the Plenum of the Supreme Court of the Russian Federation of 15.12.2022 No. 37 "On certain issues of judicial practice in criminal cases of crimes in the field of computer information, as well as other crimes committed using electronic or information and telecommunication networks, including the Internet." Russian newspaper. 2022. № 294.

[9] Federal Customs Service: Customs authorities opened over 660 criminal cases in the 1st quarter of 2025 [Electronic resource] - Access mode: - URL: https://customs.gov.ru/press/federal/document/633037.

[10] Khromenkov, I.R., Kachalova O.V. Court enforcement of legal interests in the pre-trial stages of Russian criminal proceedings: monograph. - M.: Prospect, 2023. - 176 s.

[11] The number of cybercrimes in the Russian Federation for six months of 2026 decreased by 30% [Electronic resource] - Access mode: - URL: https://www.kommersant.ru/doc/8816431.

