Научная статья

УДК 343.98

МЕТОДИКА РАССЛЕДОВАНИЯ ИНЦИДЕНТОВ, КАСАЮЩИХСЯ НЕСОБЛЮДЕНИЯ УСТАНОВЛЕННЫХ ТРЕБОВАНИЙ И ПРАВИЛ ЭКСПЛУАТАЦИИ ОБЩЕДОСТУПНЫХ СЕТЕВЫХ СИСТЕМ

Ирина Владимировна Семёнова
Академия войск национальной гвардии, Санкт-Петербург, Россия
9053202867@mail.ru

Аннотация. В условиях стремительного развития технологий и возникновения новых форм преступлений, необходимость разработки эффективных методик расследования становится как никогда актуальной. Научные исследования играют ключевую роль в адаптации правоохранительных органов к этим вызовам, предоставляя инновационные инструменты и подходы для борьбы с преступностью. От того, насколько успешно мы сможем интегрировать научные достижения в практическую деятельность, зависит безопасность общества и эффективность правосудия. В статье автором предлагается методика расследования преступления в сфере информационно-коммуникационных сетей.

Ключевые слова: преступления, расследование, должностное лицо, оператор сотовой связи, требования, правила, нарушения, методика

Для цитирования: Семёнова И.В. Методика расследования инцидентов, касающихся несоблюдения установленных требований и правил эксплуатации общедоступных сетевых систем // Вестник Военной академии войск национальной гвардии. 2025. № 1 (30).С. 73–82. URL: https://vestnik-spvi.ru/2025/03/010.pdf.

Original article

THE METHODOLOGY OF INVESTIGATION OF INCIDENTS CONCERNING NON-COMPLIANCE WITH THE ESTABLISHED REQUIREMENTS AND RULES OF OPERATION OF PUBLIC NETWORK SYSTEMS

Irina V. Semenova
Academy of the National Guard Troops, Saint-Petersburg, Russia
9053202867@mail.ru

Abstract. In the context of the rapid development of technology and the emergence of new forms of crime, the need to develop effective investigative techniques is becoming more urgent than ever. Scientific research plays a key role in adapting law enforcement agencies to these challenges by providing innovative tools and approaches to combat crime. The security of society and the effectiveness of justice depend on how successfully we can integrate scientific achievements into practical activities. In the article, the author suggests a methodology for investigating crimes in the field of information and communication networks.

Keywords*:* crimes, investigation, official, mobile operator, requirements, rules, violations, methodology

For citation: Semenova I.V. The methodology of investigation of incidents concerning non-compliance with the established requirements and rules of operation of public network systems. Vestnik Voennoj akademii vojsk nacional'noj gvardii. 2025;1(30): 73–82. (In Russ.). Available from: https://vestnik-spvi.ru/2025/03/010.pdf.

Введение

Преступления, нарушающие установленные правила, часто становятся предметом горячих обсуждений. Такая реакция общества обычно связана с тем, что данные нарушения наносят урон общественному порядку и безопасности. Когда дело доходит до открытого рассмотрения, оно может выявить недостатки в системе обеспечения законности и безопасности.

Нужно подчеркнуть, что деяния, связанные с нарушениями в области информационных технологий, представляют значительные сложности в плане их раскрытия. Это обстоятельство неизбежно приводит к тому, что процесс вынесения судебных решений может подвергаться критике как в

части применения санкций, так и в случаях их неисполнения.

Исследование

Основная проблема заключается в разделении требований и правил, а также определении непреднамеренного нанесения вреда и проведения компьютерных экспертиз. Эксперты могут сталкиваться с проблемами при определении взаимосвязи между действиями сотрудника и причинением ущерба. Законодательство не связывает уровень ответственности с серьёзностью последствий, хотя это важно для определения наказания. К примеру, если оператор не блокирует доступ к данным пользователя, которому это запрещено по закону, такое нарушение само по себе рассматривается как уголовное. В этих случаях важным является доказательство самого факта совершения преступления согласно статье 73 УПК РФ.

Также важны индивидуальные обстоятельства, приведшие к невыполнению установленных правил (согласно п. 2. ч. 1 указанного закона). В случаях, когда вред возникает в результате действий нескольких человек, и каждый из них действовал по невнимательности, ответственность за последствия должна распределяться с учетом того, насколько вклад каждого способствовал причинению ущерба. Это основывается на принципе совместного причинения.

Внесение изменений в уголовное законодательство [20, 21], устанавливающих ответственность за нарушение правил в сфере связи, представляется важным действием. Это связано с тем, что создание системы контроля с использованием средств связи соответствует стратегии информационной безопасности страны. Данная стратегия направлена на борьбу с распространением экстремистского контента, проявлениями ксенофобии и идеологией национального превосходства, которые могут подорвать государственный суверенитет, политическую и социальную стабильность, и попытки изменить конституционный строй силой. Кроме того, стратегия включает в себя противодействие внешним угрозам, осуществляемым через технические средства и информационные технологии как со стороны иностранных спецслужб и организаций, так и со стороны отдельных лиц» [7; 9; 18; С. 656].

Так, за нарушение нормативов эксплуатации оборудования связи, интегрированного с Интернетом, предусмотрены как административные, так и уголовные меры наказания. Это оборудование теперь классифицируется как инструменты для обеспечения безопасности Российской Федерации от внутренних и внешних угроз [25].

О необходимости комплексного подхода при введении уголовной ответственности за преступления говорил П. С. Дагель, подчеркивая важность учета различных факторов, таких как криминология, экономика, социополитические условия и психологические особенности. Наравне с этим следует оценивать опасность преступлений, их распространенность и динамику. Учтены должны быть альтернативные, не уголовные способы борьбы с преступностью. Законодательная система должна стремиться к созданию стабильной и эффективной сети законов, где применение криминализации и декриминализации является продуманными и сбалансированными [2, с. 57, 4].

В рамках указанной концепции установлена ответственность для индивидуальных предпринимателей и должностных лиц за нарушения в сфере использования информационных и телекоммуникационных сетей, в 2023 году статья 274.2 стала действующей нормой Уголовного Кодекса Российской Федерации [25]. Она является бланкетной, поскольку для понимания положений необходимо изучать другие нормативные правовые акты, определяющие правила установки, эксплуатации и обновления оборудования для работы в интернете, а также нормы по пропуску интернет-трафика.

Согласно ч. 1 статьи 12 Федерального закона № 126-ФЗ, принятого 7 июля 2003 года, в России действует унифицированная система связи. Эта система включает в себя несколько типов сетей, которые классифицируются в зависимости от их предназначения. В число этих сетей входят общедоступные, специализированные каналы, сети, используемые для внутренних процессов, а также предназначенные для конкретных целей.

Для создания стабильного общества, защиты основ государственного устройства и обеспечения национальной безопасности необходим контроль над информационным пространством. От мобильных операторов требуется осуществлять регулирование доступа к информации, запрещённой к распространению на территории России. Это касается сайтов, адреса которых включены в «Единый реестр» [14], а также защищённой государством информации. При обнаружении

нарушений в Интернете или сетях связи оператор должен уведомить органы правопорядка.

В целях предоставления гарантий стабильности и защиты информационной сферы, Правительство Российской Федерации установило нормы и методику ведения деятельности в сфере связи. Согласно законодательству, предоставление телекоммуникационных услуг подлежит лицензированию. Право на их предоставление имеют не только компании и частные лица, но и индивидуальные предприниматели, получившие статус операторов связи после соответствия установленным законом мерам безопасности в процессе управления сетями. Информация о таких операторах направляется в Роскомнадзор, который, в свою очередь, передает ее в службу, регулирующую радиочастоты и радиоэлектронные системы.

Несмотря на предпринятые действия, преступность в сфере цифровой информации остается на высоком уровне. Разработать универсальный метод расследования, подходящий для всех видов преступлений или нарушений в сети Интернет, невозможно. При исследовании каждого конкретного случая необходимо учитывать особенности организации, где было совершено нарушение, включая её структуру, систему отчетности и правила хранения активов. Имея эти данные, следователь может определить наиболее эффективный план расследования, который позволит достичь значимых результатов с минимальными усилиями и в кратчайшие сроки.

Следователю необходимо определить обстоятельства доступа к информации во время преступления: место, время и методы доступа, круг лиц, которые могли взаимодействовать с ней и быть причастными к преступлению, а также возможные способы скрытия преступления и его следов. Затем следует выявить конкретные детали: когда и как были совершены нарушения, кто был их исполнителем, каким образом были нарушены правила и к каким результатам это привело, как осуществлялось скрытие нарушений. Понимание механизмов преступления помогает следователю выбрать эффективные методики для его раскрытия.

Чтобы грамотно провести расследование указанных правонарушений, критически важно иметь глубокие знания о процедурах установки, правилах использования и возможностях обновления оборудования, работающего с Интернетом. Необходимо также строго следовать нормативам, касающимся обработки данных трафика [10, 12].

В области работы с информационно-коммуникационными сетями термин «порядок» обозначает четко установленную последовательность действий сотрудника, направленных на обеспечение безопасного функционирования интернет-сервисов. В соответствии с российским законодательством, отрегулированным соответствующими нормами и указаниями ведомств, этот порядок включает в себя создание мер по защите от угроз стабильности работы сетей и их мониторинг со стороны служб, отвечающих за радиочастотный спектр.

Для гарантирования стабильности и пошагового обновления сетевой структуры создается комплексный план. Его ключевые элементы включают в себя: оценку внедрения защитных механизмов; архитектуру сети; определение технических спецификаций; выбор мест для установки оборудования; требования к сетевым соединениям и их свойства; исследование распределения трафика; организацию сетевой инфраструктуры; модернизацию ключевых узлов; планы по расширению сети; программу обновления; проработку технических аспектов [12].

В соответствии с определениями, найденными в словарях [8, 19, 23], и статьей 274.2 части 2 Уголовного кодекса Российской Федерации, термин «требования» в контексте обсуждаемой области можно охарактеризовать как комплект обязательных условий для всех субъектов, организующих предоставление связи. Эти условия закреплены в законодательных актах. Они охватывают несколько главных направлений: создание системы надзора, включающей мониторинг, обнаружение нарушений и оповещение регулирующего органа, а также регистрацию при установлении связи [10].

В соответствии с установленными правилами, обязанности по использованию уникальных идентификаторов [22] и владению необходимым комплектом технических и программных средств, а также объектов связи, которые позволяют передавать трафик между различными сетями без изменений (известных как точки обмена трафиком), распространяются на компании, занимающиеся мобильной связью, а также на частных лиц и индивидуальных предпринимателей, владеющих сетями связи. Эти положения по-

могают определить статус лица, допустившего нарушение[24].

В определённых ситуациях нарушения в работе организации не приводят к ответственности сотрудников. Так, системы связи должны быть под непрерывным надзором для обеспечения их стабильности и быстрого реагирования на любые угрозы или сбои через автоматизированные управленческие системы и оперативное оповещение служб [15]. Однако если прекращение мониторинга вызвано чрезвычайными обстоятельствами, например естественными катастрофами или терактами, то это не ведёт к последствиям. В то же время игнорирование контроля из-за небрежности сотрудников, как, например, задержка в предоставлении данных о сбоях, может быть признано преступной небрежностью.

В других случаях, неосуществление такого контроля может быть результатом преступной халатности со стороны тех или иных работников (например, неоперативное предоставление информации об произошедших авариях или отказах сетей).

В технологической и научной сфере выделяют два вида причин, вызывающих сбои в работе систем. К первой категории относят те, что связаны с физическими компонентами системы, включая ошибки, допущенные персоналом, проблемы с устройствами хранения данных, программное обеспечение, предназначенное для работы в сети, и саму сетевую инфраструктуру. Во вторую категорию входят проблемы, связанные с кибератаками и экстренными ситуациями, которые могут возникнуть внезапно и повлиять на стабильность систем [6].

Пренебрежение правилами мониторинга интернет-трафика может проявляться как в задержке определения потенциальных угроз, так и в отсутствии современных средств обеспечения кибербезопасности. Обнаружение нарушения – это лишь начальный этап расследования. Далее дознавателю предстоит выяснить обстоятельства и характер данного инцидента, а также определить, было ли нарушение случайностью или результатом предумышленных действий.

Для обеспечения честности процесса разбирательства ключевую роль играет непредвзятость следствия. Субъект расследования обязан руководствоваться фактами, внимательно относясь к материалам, представляемым обеими сторонами – защитой и обвинением. Это особенно актуально в ситуациях, когда обвиняемые отрицают свою виновность и создают препятствия в работе правоохранительных органов. Закон и беспристрастность должны быть основой действий следственной группы [28].

Основное отличие между понятиями «порядок» и «требования» заключается в следующем. «Порядок» связан с выполнением определённых действий в конкретной последовательности. Несоблюдение этой последовательности может привести к негативным последствиям. Например, если не обновить системы безопасности вовремя, исходя из предполагаемых рисков, это может стать причиной утечки цифровой информации или сбоев в работе цифровых систем, что в свою очередь нанесёт материальный вред.

В данном случае происходит нарушение установленных норм, выражающееся в невозможности зафиксировать сведения о пользователях или их контактных данных, которые применяются сетью в процессе обмена информацией.

При анализе преступлений, связанных с нарушением установленных норм и правил, важно учитывать начальные этапы расследования, поскольку они отличаются в зависимости от характера нарушения. Когда речь идет о несоблюдении определенного порядка, особое внимание уделяется лицам, ответственным за организацию данного процесса. В этом контексте акцент делается на операторов связи, обладающих полномочиями для поддержания стабильной и безопасной работы сетей, а также на сотрудников, в задачи которых входит защита от цифровых угроз с помощью специализированного оборудования.

Если в процессе контроля за действиями, связанными с техническими средствами, выясняется, что оборудование функционирует неправильно или не предпринимаются меры против киберугроз, что приводит к проблемам в работе телекоммуникационной сети (к примеру, уменьшение пропускной способности или вред системе защиты вызывает падение скорости связи), начальная стадия расследования направлена на конкретное лицо или группу лиц. Эти индивиды или группы изначально были ответственны за надлежащее функционирование этих систем и могли допустить возникновение такой проблемы.

При расследовании инцидентов, связанных с нарушением определённых норм, часто бывает сложно сразу установить виновных. Для выявления лиц, ответственных за

эти нарушения, дознавателям придется анализировать улики. Нормы, регулирующие работу сетевых систем, утверждаются официальными документами. Владельцы систем должны первыми применять эти нормы, но в их повседневной эксплуатации участвуют также диспетчерские службы. Для того чтобы выяснить источник проблемы, следует обращаться к записям и электронным данным, связанным с инцидентом.

Подходы к проведению следствия значительно различаются в зависимости от обстоятельств нарушений. Когда дело касается лиц, чья должностная роль напрямую связана с управлением определённой сферой, ключевым аспектом становится детальный анализ действий сотрудников, задействованных в управленческих процессах. В ситуациях, когда происходит нарушение установленных норм, первоочередное значение приобретает тщательный осмотр места происшествия, который заложит основу для разработки дальнейшей стратегии следствия.

Действия, нарушающие положения частей 1 и 2 ст. 274.2 Уголовного кодекса Российской Федерации, объединены одной характеристикой: вред, нанесенный законным процессам функционирования государственных или общественных структур, является результатом неправомерных деяний (или промедления) лиц, занимающих ответственные посты.

Цифровые преступления затрагивают права и интересы личности, общества и государства, которые защищены законом. При наличии достаточных оснований, определенных статьей 140 Уголовно-процессуального кодекса Российской Федерации, включая результаты аудита, данные внутренних расследований, обращения граждан или отчеты СМИ, может быть возбуждено уголовное дело.

В ходе методики изучения преступных действий акцент сделан на сбор информации о роли участника событий, его обязанностях и сути его неправомерных действий; оценке ущерба, нанесенного его деяниями; установлении причинно-следственных связей. При этом ответственность личности определяется на основании ее активных действий или пассивности, которые повлекли за собой конкретные неблагоприятные итоги.

Необходимо установить, имеется ли связь между неправомерными действиями лица и нарушениями в сфере IT. Ключевым аспектом успешного проведения следствия является способность исследователя выделить уникальные признаки преступления.

Для всестороннего анализа деятельности компании, особенно когда дело касается расследования преступлений, связанных с должностными проступками, крайне важно тщательно исследовать несколько ключевых аспектов: климат внутри команды и установленные правила поведения; нормативные акты и иные документы, устанавливающие границы ответственности сотрудников; специфика работы с корпоративной документацией. Эти элементы помогут получить полное представление о внутренней среде предприятия и могут выявить потенциальные слабые места, где возможны нарушения.

В начале расследования преступлений особое значение приобретают первичные материалы, которые служат основой для выявления информации о правонарушениях. В случаях нарушений в сфере связи первым шагом часто является анализ и конфискация документации. Именно на начальных этапах важность бумажных носителей как доказательств возрастает, требуя детального внимания при их рассмотрении. Процесс запроса документов для получения информации может быть менее эффективен, поскольку пропадает возможность непосредственного наблюдения за их хранением, что увеличивает шансы на утрату или фальсификацию важнейших сведений.

Для обеспечения контроля за потоками данных необходимы определённые знания. Нужно проводить аудит транзита информации с помощью устройств для нейтрализации угроз (УНУ). Критично важно фильтрование информационных потоков, обеспечение их защиты, а также анализ собранных данных и подготовка соответствующих отчётов.

Заключение

Таким образом, важно подчеркнуть, что начальный этап расследования преступлений тесно связан с теоретическим пониманием особенностей действующей нормы. Анализ характеристик и процессов, лежащих в основе преступного поведения, имеет критическое значение не только для теории криминалистики, но и для реальной практики обнаружения и прекращения преступлений [1, 29].

Понимание различий в процедурах монтажа, использования и критериях, которые ставятся перед пропуском данных, имеет критическое значение с точки зрения законодательства для определения характера правонарушения.

Список источников

1. Бессонов А. А. О некоторых современных методах изучения преступлений в криминалистике // Сборник Всероссийской научно-практической конференции «Криминалистика и новые вызовы современности» (58-е криминалистические чтения). М., 2018. 400 с.

2. Дагель П. С. Проблемы советской уголовной политики. Владивосток, 1982. 124 с.

3. Земцов А. Н. Моделирование и оценка показателей надежности и отказоустойчивости систем связи / А. Н. Земцов, Р. С. Ньяти // ИВД. 2019. №5 (56). URL: https://cyberleninka.ru/article/n/modelirovanie-i-otsenka-pokazateley-nadezhnosti-i-otkazoustoychivosti-sistem-svyazi (дата обращения: 19.05.2024).

4. Кибальник А. Г. Недопустимость административной преюдиции в уголовном законодательстве // Библиотека криминалиста. 2013. № 2(7). С. 119–125.

5. Лопашенко Н. А. Административной преюдиции в уголовном праве – нет! // Вестник Академии Генеральной прокуратуры Российской Федерации. 2011. № 3(23). С. 64–71.

6. Манукян М. С. Классификация сетевых отказов телекоммуникационных сетей // Вестник МГУП. 2011. № 1. С. 149–155.

7. Нудель С. Л. Модернизация уголовной политики: проблемы правового регулирования // Журнал российского права. 2023. № 1. С. 9.

8. Ожегов С. И. Толковый словарь русского языка: 72500 слов и 7500 фразеологических выражений. 2-е изд., испр. и доп. / С. И. Ожегов, Н. Ю. Шведова. М. : Азъ, 1994. 907 с.

9. Паспорт проекта Федерального закона № 130406-8 «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации» (в целях совершенствования уголовно-правовой охраны национальных интересов Российской Федерации, прав и свобод граждан от новых форм преступной деятельности и угроз государственной безопасности)» // (внесен депутатами Государственной Думы ФС РФ В. И. Пискаревым, Э. А. Валеевым, А. В. Картаполовым, А. Л. Красовым, А. Б. Выборным)» (подписан Президентом Российской Федерации). Опубликован не был.

10. Постановление Правительства Российской Федерации от 03 ноября 2022 г. № 1978 «Об утверждении требований к системе обеспечения соблюдения операторами связи требований при оказании услуг связи и услуг по пропуску трафика в сети связи общего пользования и Правил функционирования и взаимодействия системы обеспечения соблюдения операторами связи требований при оказании услуг связи и услуг по пропуску трафика в сети связи общего пользования с информационными системами и иными системами, в том числе с системами операторов связи» // Собрание законодательства Российской Федерации. 2022. № 46. Ст. 7995.

11. Постановление Правительства Российской Федерации от 03 ноября 2022 г. № 1978 «Об утверждении требований к системе обеспечения соблюдения операторами связи требований при оказании услуг связи и услуг по пропуску трафика в сети связи общего пользования и Правил функционирования и взаимодействия системы обеспечения соблюдения операторами связи требований при оказании услуг связи и услуг по пропуску трафика в сети связи общего пользования с информационными системами и иными системами, в том числе с системами операторов связи» // Собрание законодательства. 2022. № 46. Ст. 7995.

12. Постановление Правительства Российской Федерации от 12 декабря 2020 г. № 126 «Об установке, эксплуатации и о модернизации в сети связи оператора связи технических средств противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети "Интернет" и сети связи общего пользования» (вместе с «Правилами установки, эксплуатации и модернизации в сети связи оператора связи технических средств противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования») // Собрание законодательства Российской Федерации. 2020. № 8. Ст. 1001.

13. Постановление Правительства Российской Федерации от 12.02.2020 г. № 126 «Об установке, эксплуатации и о модернизации в сети связи оператора связи технических средств противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования» (вместе с «Правилами установки, эксплуатации и модернизации в сети связи оператора связи технических средств противодействия угрозам

устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования») // Собрание законодательства Российской Федерации. 2020. № 8. Ст. 1001.

14. Постановление Правительства Российской Федерации от 26 октября 2012 г. № 1101 «О единой автоматизированной информационной системе «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено» (вместе с «Правилами создания, формирования и ведения единой автоматизированной информационной системы «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено», «Правилами принятия уполномоченными Правительством Российской Федерации федеральными органами исполнительной власти решений в отношении отдельных видов информации и материалов, распространяемых посредством информационно-телекоммуникационной сети «Интернет», распространение которых в Российской Федерации запрещено») // Российская газета. 2012. № 249.

15. Приказ Минкомсвязи России от 10 октября 2019 г. № 582 «Об утверждении требований к функционированию систем управления сетями связи при возникновении угроз устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования» // Официальный интернет-портал правовой информации. URL: http://www.pravo.gov.ru (дата обращения:15.01.2020).

16. Приказ Минкомсвязи России от 10 октября 2019 г. № 582 «Об утверждении требований к функционированию систем управления сетями связи при возникновении угроз устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования» // Официальный интернет-портал правовой информации. URL:http://www.pravo.gov.ru, (дата обращения: 15.01.2020).

17. Решетников А. Ю. Уголовный проступок и неоконченное преступление: точки соприкосновения // Уголовное право. 2017. № 4. С. 104–108.

18. Русскевич Е. А. Нарушение правил централизованного управления техническими средствами противодействия угрозам информационной безопасности // Journal of Digital Technologies and Law. 2023. № 3. С. 650–672.

19. Толковый словарь русского языка: Ок. 700 слов. ст.: Свыше 6000 значений / под ред. Д. В. Дмитриева. М. : Астрель, 2003. 782 с.

20. Указ Президента Российской Федерации от 02 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» // Собрание законодательства Российской Федерации. 2021. № 27 (Ч. II). Ст. 5351.

21. Указ Президента Российской Федерации от 05 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства Российской Федерации. 2016. № 50. Ст. 7074.

22. Уникальный идентификатор средства связи или иного технического средства в информационно-телекоммуникационной сети «Интернет». URL: https://69.rkn.gov.ru/news/news276078.htm. (дата обращения: 19.05.2024).

23. Ушаков Д. Н. Большой толковый словарь русского языка: современная редакция. М. : Дом Славянской кн., 2008. 959 с.

24. Федеральный закон от 07 июля 2003 г. № 126-ФЗ «О связи» п. 28.5 Ст. 2 // Собрание законодательства Российской Федерации. 2003. № 28. Ст. 2895.

25. Федеральный закон от 14 июля 2022 г. № 260-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации» // Собрание законодательства Российской Федерации. 2022. № 29 (Ч. II). Ст. 5227.

26. Философская энциклопедия. URL: https://dic.academic.ru/dic.nsf/enc_philosophy/3040 (дата обращения: 19.05.2024).

27. Хадыма Р. и Фелс Деборх И. Причины отказов в информационно-технологических телекоммуникационных сетях / пер. с англ. В. В. Тараненко. URL: http://www.docstoc.com/docs/3944884/Causes-of-Failure-in-Information-Technology-Telecommunications-/ https://cyberleninka.ru/article/n/klassifikatsiya-setevyh-otkazov-

telekommunikatsionnyh-setey (дата обращения: 19.05.2024).

28. Халиков А. Н. Перспективы развития криминалистической методики расследования // Вестник УЮИ. 2020. № 3 (89). С. 127–133.

29. Халиков А. Н. Применение общих положений методики расследования в отношении новых составов преступлений, криминализованных уголовным законом // Российский следователь. 2023. № 6. С. 2–6.

References

1. Bessonov A. A. O nekotoryh sovremennyh metodah izucheniya prestuplenij v kriminalistike // Sbornik Vserossijskoj nauchno-prakticheskoj konferencii «Kriminalistika i novye vyzovy sovremennosti» (58-e kriminalisticheskie chteniya). M., 2018. 400 s. (In Russ.).

2. Dagel' P. S. Problemy sovetskoj ugolovnoj politiki. Vladivostok, 1982. 124 s. (In Russ.).

3. Zemcov A. N. Modelirovanie i ocenka pokazatelej nadezhnosti i otkazoustojchivosti sistem svyazi / A. N. Zemcov, R. S. N'yati // IVD. 2019;5 (56). Available from: https://cyberleninka.ru/article/n/modelirovanie-i-otsenka-pokazateley-nadezhnosti-i-otkazoustoychivosti-sistem-svyazi (data obrashcheniya: 19.05.2024). (In Russ.).

4. Kibal'nik A. G. The inadmissibility of administrative prejudice in criminal law // Biblioteka kriminalista. 2013;2(7): 119–125. (In Russ.).

5. Lopashenko N. A. There is no administrative prejudice in criminal law! // Vestnik Akademii General'noj prokuratury Rossijskoj Federacii. 2011;3(23): 64–71. (In Russ.).

6. Manukyan M. S. Classification of network failures of telecommunication networks // Vestnik MGUP. 2011;1: 149–155. (In Russ.).

7. Nudel' S. L. Modernization of criminal policy: problems of legal regulation // ZHurnal rossijskogo prava. 2023;1: 9. (In Russ.).

8. Ozhegov S. I. Tolkovyj slovar' russkogo yazyka: 72500 slov i 7500 frazeologicheskih vyrazhenij. 2-e izd., ispr. i dop. / S. I. Ozhegov, N. YU. SHvedova. M. : Az", 1994. 907 s. (In Russ.).

9. Pasport proekta Federal'nogo zakona № 130406-8 «O vnesenii izmenenij v Ugolovnyj kodeks Rossijskoj Federacii i Ugolovno-processual'nyj kodeks Rossijskoj Federacii» (v celyah sovershenstvovaniya ugolovno-pravovoj ohrany nacional'nyh interesov Rossijskoj Federacii, prav i svobod grazhdan ot novyh form prestupnoj deyatel'nosti i ugroz gosudarstvennoj bezopasnosti)» // (vnesen deputatami Gosudarstvennoj Dumy FS RF V. I. Piskarevym, E. A. Valeevym, A. V. Kartapolovym, A. L. Krasovym, A. B. Vybornym)» (podpisan Prezidentom Rossijskoj Federacii). Opublikovan ne byl. (In Russ.).

10. Postanovlenie Pravitel'stva Rossijskoj Federacii ot 03 noyabrya 2022 g. № 1978 «Ob utverzhdenii trebovanij k sisteme obespecheniya soblyudeniya operatorami svyazi trebovanij pri okazanii uslug svyazi i uslug po propusku trafika v seti svyazi obshchego pol'zovaniya i Pravil funkcionirovaniya i vzaimodejstviya sistemy obespecheniya soblyudeniya operatorami svyazi trebovanij pri okazanii uslug svyazi i uslug po propusku trafika v seti svyazi obshchego pol'zovaniya s informacionnymi sistemami i inymi sistemami, v tom chisle s sistemami operatorov svyazi» // Sobranie zakonodatel'stva Rossijskoj Federacii. 2022. № 46. St. 7995. (In Russ.).

11. Postanovlenie Pravitel'stva Rossijskoj Federacii ot 03 noyabrya 2022 g. № 1978 «Ob utverzhdenii trebovanij k sisteme obespecheniya soblyudeniya operatorami svyazi trebovanij pri okazanii uslug svyazi i uslug po propusku trafika v seti svyazi obshchego pol'zovaniya i Pravil funkcionirovaniya i vzaimodejstviya sistemy obespecheniya soblyudeniya operatorami svyazi trebovanij pri okazanii uslug svyazi i uslug po propusku trafika v seti svyazi obshchego pol'zovaniya s informacionnymi sistemami i inymi sistemami, v tom chisle s sistemami operatorov svyazi» // Sobranie zakonodatel'stva. 2022. № 46. St. 7995. (In Russ.).

12. Postanovlenie Pravitel'stva Rossijskoj Federacii ot 12 dekabrya 2020 g. № 126 «Ob ustanovke, ekspluatacii i o modernizacii v seti svyazi operatora svyazi tekhnicheskih sredstv protivodejstviya ugrozam ustojchivosti, bezopasnosti i celostnosti funkcionirovaniya na territorii Rossijskoj Federacii informacionno-telekommunikacionnoj seti "Internet" i seti svyazi obshchego pol'zovaniya» (vmeste s «Pravilami ustanovki, ekspluatacii i modernizacii v seti svyazi operatora svyazi tekhnicheskih sredstv protivodejstviya ugrozam ustojchivosti, bezopasnosti i celostnosti funkcionirovaniya na territorii Rossijskoj Federacii informacionno-telekommunikacionnoj seti «Internet» i seti svyazi obshchego pol'zovaniya») // Sobranie zakonodatel'stva Rossijskoj Federacii. 2020. № 8. St. 1001. (In Russ.).

13. Postanovlenie Pravitel'stva Rossijskoj Federacii ot 12.02.2020 g. № 126 «Ob ustanovke, ekspluatacii i o modernizacii v seti svyazi operatora svyazi tekhnicheskih sredstv protivodejstviya ugrozam ustojchivosti, bezopasnosti i celostnosti funkcionirovaniya na territorii Rossijskoj Federacii

informacionno-telekommunikacionnoj seti «Internet» i seti svyazi obshchego pol'zovaniya» (vmeste s «Pravilami ustanovki, ekspluatacii i modernizacii v seti svyazi operatora svyazi tekhnicheskih sredstv protivodejstviya ugrozam ustojchivosti, bezopasnosti i celostnosti funkcionirovaniya na territorii Rossijskoj Federacii informacionno-telekommunikacionnoj seti «Internet» i seti svyazi obshchego pol'zovaniya») // Sobranie zakonodatel'stva Rossijskoj Federacii. 2020. № 8. St. 1001. (In Russ.).

14. Postanovlenie Pravitel'stva Rossijskoj Federacii ot 26 oktyabrya 2012 g. № 1101 «O edinoj avtomatizirovannoj informacionnoj sisteme «Edinyj reestr domennyh imen, ukazatelej stranic sajtov v informacionno-telekommunikacionnoj seti «Internet» i setevyh adresov, pozvolyayushchih identificirovat' sajty v informacionno-telekommunikacionnoj seti «Internet», soderzhashchie informaciyu, rasprostranenie kotoroj v Rossijskoj Federacii zapreshcheno» (vmeste s «Pravilami sozdaniya, formirovaniya i vedeniya edinoj avtomatizirovannoj informacionnoj sistemy «Edinyj reestr domennyh imen, ukazatelej stranic sajtov v informacionno-telekommunikacionnoj seti «Internet» i setevyh adresov, pozvolyayushchih identificirovat' sajty v informacionno-telekommunikacionnoj seti «Internet», soderzhashchie informaciyu, rasprostranenie kotoroj v Rossijskoj Federacii zapreshcheno», «Pravilami prinyatiya upolnomochennymi Pravitel'stvom Rossijskoj Federacii federal'nymi organami ispolnitel'noj vlasti reshenij v otnoshenii otdel'nyh vidov informacii i materialov, rasprostranyaemyh posredstvom informacionno-telekommunikacionnoj seti «Internet», rasprostranenie kotoryh v Rossijskoj Federacii zapreshcheno») // Rossijskaya gazeta. 2012. № 249. (In Russ.).

15. Prikaz Minkomsvyazi Rossii ot 10 oktyabrya 2019 g. № 582 «Ob utverzhdenii trebovanij k funkcionirovaniyu sistem upravleniya setyami svyazi pri vozniknovenii ugroz ustojchivosti, bezopasnosti i celostnosti funkcionirovaniya na territorii Rossijskoj Federacii informacionno-telekommunikacionnoj seti «Internet» i seti svyazi obshchego pol'zovaniya» // Oficial'nyj internet-portal pravovoj informacii. URL: http://www.pravo.gov.ru (data obrashcheniya:15.01.2020). (In Russ.).

16. Prikaz Minkomsvyazi Rossii ot 10 oktyabrya 2019 g. № 582 «Ob utverzhdenii trebovanij k funkcionirovaniyu sistem upravleniya setyami svyazi pri vozniknovenii ugroz ustojchivosti, bezopasnosti i celostnosti funkcionirovaniya na territorii Rossijskoj Federacii informacionno-telekommunikacionnoj seti «Internet» i seti svyazi obshchego pol'zovaniya» // Oficial'nyj internet-portal pravovoj informacii. URL:http://www.pravo.gov.ru, (data obrashcheniya: 15.01.2020). (In Russ.).

17. Reshetnikov A. YU. A criminal offense and an unfinished crime: points of contact // Ugolovnoe pravo. 2017;4: 104–108. (In Russ.).

18. Russkevich E. A. Narushenie pravil centralizovannogo upravleniya tekhnicheskimi sredstvami protivodejstviya ugrozam informacionnoj bezopasnosti // Journal of Digital Technologies and Law. 2023;3: 650–672. (In Russ.).

19. Tolkovyj slovar' russkogo yazyka: Ok. 700 slov. st.: Svyshe 6000 znachenij / pod red. D. V. Dmitrieva. M. : Astrel', 2003. 782 s. (In Russ.).

20. Ukaz Prezidenta Rossijskoj Federacii ot 02 iyulya 2021 g. № 400 «O Strategii nacional'noj bezopasnosti Rossijskoj Federacii» // Sobranie zakonodatel'stva Rossijskoj Federacii. 2021. № 27 (CH. II). St. 5351. (In Russ.).

21. Ukaz Prezidenta Rossijskoj Federacii ot 05 dekabrya 2016 g. № 646 «Ob utverzhdenii Doktriny informacionnoj bezopasnosti Rossijskoj Federacii» // Sobranie zakonodatel'stva Rossijskoj Federacii. 2016. № 50. St. 7074. (In Russ.).

22. Unikal'nyj identifikator sredstva svyazi ili inogo tekhnicheskogo sredstva v informacionno-telekommunikacionnoj seti «Internet». URL: https://69.rkn.gov.ru/news/news276078.htm. (data obrashcheniya: 19.05.2024). (In Russ.).

23. Ushakov D. N. Bol'shoj tolkovyj slovar' russkogo yazyka: sovremennaya redakciya. M. : Dom Slavyanskoj kn., 2008. 959 s. (In Russ.).

24. Federal'nyj zakon ot 07 iyulya 2003 g. № 126-FZ «O svyazi» p. 28.5 St. 2 // Sobranie zakonodatel'stva Rossijskoj Federacii. 2003. № 28. St. 2895. (In Russ.).

25. Federal'nyj zakon ot 14 iyulya 2022 g. № 260-FZ «O vnesenii izmenenij v Ugolovnyj kodeks Rossijskoj Federacii i Ugolovno-processual'nyj kodeks Rossijskoj Federacii» // Sobranie zakonodatel'stva Rossijskoj Federacii. 2022. № 29 (CH. II). St. 5227. (In Russ.).

26. Filosofskaya enciklopediya. URL: https://dic.academic.ru/dic.nsf/enc_philosophy/3040 (data obrashcheniya: 19.05.2024). (In Russ.).

27. Hadyma R. i Fels Deborh I. Prichiny otkazov v informacionno-tekhnologicheskih telekommunikacionnyh setyah / per. s angl. V. V. Taranenko. URL: http://www.docstoc.com/docs/3944884/Causes-of-Failure-in-Information-Technology-

Telecommunications-/ https://cyberleninka.ru/article/n/klassifikatsiya-setevyh-otkazov-telekommunikatsionnyh-setey (data obrashcheniya: 19.05.2024). (In Russ.).

28. Halikov A. N. Prospects for the development of forensic investigation techniques // Vestnik UYUI. 2020;3 (89): 127–133. (In Russ.).

29. Halikov A. N. Application of the general provisions of the investigation methodology in relation to new types of crimes criminalized by criminal law // Rossijskij sledovatel'. 2023;6: 2–6. (In Russ.).

Информация об авторах

И. В. Семёнова *– кандидат юридических наук*

Статья поступила в редакцию 04.02.2025;
одобрена после рецензирования 15.03.2025;
принята к публикации 20.03.2025.

Information about the authors

I. V. Semyonova *– Candidate of Sciences (Law)*

The article was submitted 04.02.2025;
approved after reviewing 15.03.2025;
accepted for publication 20.03.2025.