Научная статья
УДК 343.3/.7
DOI: 10.47475/2311-696X-2026-50-3-189-195

С. 189–195

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ОБЪЕКТА И ПРЕДМЕТА ПРЕСТУПЛЕНИЯ, ПРЕДУСМОТРЕННОГО СТАТЬЕЙ 274.3 УК РФ

Сергей Владимирович Кравчук

Казанский инновационный университет имени В. Г. Тимирясова (ИЭУП), г. Казань, Россия
9836565@mail.ru

Аннотация. В статье проводится исследование объекта и предмета преступления, предусмотренного ст. 274³ УК РФ, устанавливающей ответственность за незаконное использование абонентского терминала пропуска трафика или виртуальной телефонной станции. Автор осуществляет многоуровневый анализ объекта преступления, выделяя родовой, видовой и непосредственный объекты посягательства, обосновывает принадлежность данного состава к преступлениям в сфере компьютерной информации. Исследуются дискуссионные вопросы определения основного непосредственного объекта, на который посягает незаконное использование телекоммуникационного оборудования. Особое внимание уделяется детальному изучению предмета преступления — абонентского терминала пропуска трафика и виртуальной телефонной станции, их технических характеристик, функционального назначения и юридически значимых признаков. Предложена классификация предмета преступления, критерии отграничения противоправных устройств от легального телекоммуникационного оборудования. Обосновывается вывод о сложном многообъектном характере преступления и необходимости системного толкования признаков предмета с учетом технической специфики телекоммуникационного оборудования и целей уголовно-правовой охраны.

Ключевые слова: объект преступления, предмет преступления, абонентский терминал пропуска трафика, виртуальная телефонная станция, телекоммуникационное оборудование, общественные отношения, компьютерная информация, информационная безопасность, квалификация преступлений, уголовная ответственность

Для цитирования: Кравчук С. В. Актуальные проблемы объекта и предмета преступления, предусмотренного статьей 274.3 УК РФ // Правопорядок: история, теория, практика. 2026. № 3 (50). С. 189–195. DOI: 10.47475/2311-696X-2026-50-3-189-195

Research article

CURRENT ISSUES RELATED TO THE OBJECT AND THE SUBJECT OF THE CRIME, PROVIDED FOR IN ARTICLE 274³ OF THE CRIMINAL CODE OF THE RUSSIAN FEDERATION

Sergey V. Kravchuk

Kazan Innovative University named after V. G. Timiryasov (IEPU), Kazan, Russia
9836565@mail.ru

Abstract. The article examines the object and subject of the crime provided for in Article 274³ of the Criminal Code of the Russian Federation, which establishes liability for the illegal use of a subscriber's traffic terminal or virtual telephone exchange. The author carries out a multilevel analysis of the object of the crime, identifying generic, specific and direct objects of encroachment, justifies the affiliation of this composition to crimes in the field of computer information. The debatable issues of defining the main direct object and optional objects that are encroached upon by the illegal use of telecommunication equipment are investigated. Special attention is paid to a detailed study of the subject of the crime — the subscriber terminal for traffic access and the virtual telephone exchange, their technical characteristics, functional purpose and legally significant features. A classification of the subject of the crime and criteria for distinguishing illegal devices from legal telecommunications equipment are proposed. The author substantiates the conclusion about the complex multi-objective nature of the crime and the need for a systematic interpretation of the signs of the subject, taking into account the technical specifics of telecommunications equipment and the goals of criminal law protection.

© Кравчук С. В.

Keywords: object of crime, subject of crime, subscriber terminal for passing traffic, virtual telephone exchange, telecommunication equipment, public relations, computer information, information security, qualification of crimes, criminal liability.

For citation: Kravchuk SV. Current Issues Related to the Object and the Subject of the Crime, Provided for in Article 274.3 of the Criminal Code of the Russian Federation. *Pravoporyadok: istoriya, teoriya, praktika* [Legal and Order: History, Theory, Practice]. 2026;(3):189-195. (In Russ.). DOI: 10.47475/2311-696X-2026-50-3-189-195

Введение

Введение в Уголовный кодекс Российской Федерации (далее — УК РФ) ст. 274[3], устанавливающей уголовную ответственность за незаконное использование абонентского терминала пропуска трафика или виртуальной телефонной станции, актуализировало фундаментальную доктринальную задачу определения объекта и предмета данного преступления как основополагающих элементов состава, определяющих социально-правовую природу криминализированного деяния, его место в системе Особенной части УК РФ и критерии разграничения со смежными составами преступлений. Предмет преступления в рассматриваемом составе приобретает особое значение, поскольку специфика технических устройств определяет возможность квалификации деяния по ст. 274[3] УК РФ.

Системное расположение ст. 274[3] в гл. 28 УК РФ «Преступления в сфере компьютерной информации» предопределяет родовой и видовой объекты посягательства, однако вызывает дискуссионные вопросы относительно обоснованности такой законодательной систематизации с учетом специфики охраняемых общественных отношений и механизма причинения вреда. Определение непосредственного объекта преступления требует детального анализа социальной природы общественных отношений, нарушаемых незаконным использованием телекоммуникационного оборудования, и соотношения различных охраняемых интересов, одновременно страдающих от данного вида преступной деятельности. Предмет преступления в виде абонентского терминала пропуска трафика или виртуальной телефонной станции представляет собой сложные технические устройства, юридическое определение которых требует интеграции правовых и технических подходов [3, с. 255–256], выработки критериев отграничения противоправных устройств от легального телекоммуникационного оборудования, используемого в правомерных целях.

Родовой и видовой объекты преступления: дискуссионные вопросы

Определение родового и видового объектов преступления, предусмотренного ст. 274[3] УК РФ, основывается на системном анализе места данной нормы в структуре Особенной части УК РФ и выявлении общих признаков группы преступлений, объединенных законодателем в соответствующий раздел и главу. Ст. 274[3] УК РФ включена в гл. 28 УК РФ «Преступления в сфере компьютерной информации», входящую в разд. IX «Преступления против общественной безопасности и общественного порядка». Следовательно, родовым объектом преступления выступают общественные отношения в сфере обеспечения общественной безопасности и общественного порядка как совокупность устойчивых социальных связей, обеспечивающих нормальные условия жизнедеятельности общества, безопасное функционирование социальных институтов, защищенность жизненно важных интересов личности, общества и государства от различных угроз [4].

Общественная безопасность в широком смысле представляет собой состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз, при котором обеспечивается реализация конституционных прав и свобод граждан, достойное качество и уровень их жизни, суверенитет, независимость, государственная и территориальная целостность, устойчивое социально-экономическое развитие Российской Федерации [1]. Преступления против общественной безопасности характеризуются многообъектностью посягательства, способностью причинять вред неопределенному кругу лиц, социально значимым объектам и процессам, общественным отношениям, обеспечивающим нормальные условия функционирования общества. Включение незаконного использования абонентского терминала пропуска трафика в систему преступлений против общественной безопасности отражает законодательное признание того, что данное деяние создает угрозу не только индивидуальным правоохраняемым интересам конкретных потерпевших, но и безопасности функционирования телекоммуникационной инфраструктуры как элемента критически важной инфраструктуры государства и общества.

Видовым объектом преступления, предусмотренного ст. 274[3] УК РФ, выступают общественные отношения в сфере обеспечения безопасности компьютерной информации как более узкая группа общественных отношений, охраняемых нормами гл. 28 УК РФ. Законодательное определение понятия «компьютерная информация» содержится в ст. 272 УК РФ. Данное определение охватывает широкий спектр информационных объектов, циркулирующих в информационно-телекоммуникационных системах, включая данные, передаваемые по сетям связи, информацию, обрабатываемую компьютерными системами, сведения, хранящиеся в электронной форме. Вместе с тем, отнесение незаконного использования абонентского терминала пропуска трафика к преступлениям в сфере компьютерной информации представляется дискуссионным и требует критического осмысления.

© Кравчук С. В.

Традиционное понимание преступлений в сфере компьютерной информации связывает их с неправомерным воздействием на компьютерную информацию как предмет преступления. Общим признаком данных преступлений выступает направленность деяния на нарушение конфиденциальности, целостности или доступности компьютерной информации [6, с. 151]. Однако незаконное использование абонентского терминала пропуска трафика не обязательно связано с воздействием на компьютерную информацию, нарушением ее защиты или модификацией содержания. Основное содержание общественной опасности данного деяния заключается в создании технических условий для совершения иных преступлений, прежде всего дистанционных мошенничеств, посредством злоупотребления легальными функциями телекоммуникационного оборудования [2, с. 136].

Критический анализ системного расположения ст. 274[3] УК РФ позволяет констатировать определенную условность включения данной нормы в главу о преступлениях в сфере компьютерной информации. Незаконное использование абонентского терминала пропуска трафика ближе к преступлениям, связанным с нарушением установленного порядка функционирования телекоммуникационной инфраструктуры и злоупотреблением техническими возможностями современных средств связи. Альтернативным вариантом систематизации могло бы стать включение данной нормы в гл. 22 УК РФ «Преступления в сфере экономической деятельности» как специальной нормы об ответственности за незаконное предпринимательство в сфере оказания услуг связи либо формирование самостоятельной главы о преступлениях против безопасности функционирования информационно-телекоммуникационной инфраструктуры. Вместе с тем, законодательное решение о включении ст. 274[3] в гл. 28 УК РФ предопределяет необходимость определения видового объекта как общественных отношений в сфере безопасности компьютерной информации с расширительным толкованием данного понятия, охватывающим безопасность функционирования информационно-телекоммуникационной инфраструктуры.

Непосредственный объект преступления

Определение непосредственного объекта преступления, предусмотренного ст. 274[3] УК РФ, представляет собой наиболее сложную доктринальную задачу, требующую выявления конкретных общественных отношений, на которые направлено посягательство и которым причиняется вред в результате совершения преступления. Анализ диспозиции ст. 274[3] УК РФ и социальной природы криминализированного деяния свидетельствует о сложном многообъектном характере преступления, одновременно посягающего на несколько групп охраняемых общественных отношений. Непосредственным основным объектом следует признать общественные отношения, обеспечивающие установленный нормативными правовыми актами порядок использования телекоммуникационного оборудования и абонентских номеров в сетях связи. Данные отношения регулируются Федеральным законом от 7 июля 2003 г. № 126-ФЗ «О связи»[1], нормативными правовыми актами в области связи, правилами оказания услуг связи, техническими регламентами и стандартами.

Содержание указанных общественных отношений составляет деятельность по обеспечению законного, безопасного и эффективного функционирования телекоммуникационной инфраструктуры как критически важного элемента современного информационного общества. Субъектами данных отношений выступают государство в лице уполномоченных органов регулирования в сфере связи, операторы связи, пользователи услугами связи, производители и поставщики телекоммуникационного оборудования. Государство устанавливает правила функционирования телекоммуникационной инфраструктуры, выдает лицензии на осуществление деятельности в области оказания услуг связи, утверждает порядок применения абонентских номеров, определяет технические требования к оборудованию. Операторы связи обязаны соблюдать лицензионные требования, обеспечивать качество и безопасность услуг связи, предоставлять возможность проведения оперативно-розыскных мероприятий. Пользователи услугами связи наделяются правом на получение качественных услуг связи и несут обязанность соблюдать правила пользования услугами связи, не допускать использования услуг связи в противоправных целях.

Незаконное использование абонентского терминала пропуска трафика или виртуальной телефонной станции нарушает установленный публично-правовой порядок функционирования телекоммуникационной инфраструктуры посредством осуществления деятельности по оказанию услуг связи без соответствующей лицензии, использования абонентских номеров способами, не предусмотренными условиями их выделения, создания технических препятствий для проведения оперативно-розыскных мероприятий, искажения идентификаторов вызывающих абонентов. Данные действия дестабилизируют нормальное функционирование сетей связи, создают избыточную нагрузку на телекоммуникационную инфраструктуру, препятствуют осуществлению государственного контроля и надзора, подрывают доверие граждан к институту телефонной связи как средству безопасной коммуникации. Следовательно, непосредственным основным объектом преступления выступают общественные отношения, обеспечивающие установленный порядок использования средств связи и функционирования телекоммуникационной инфраструктуры.

Дополнительным непосредственным объектом преступления, на который посягает незаконное использование абонентского терминала пропуска трафика,

[1] Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи» // Собрание законодательства Российской Федерации. 2003. № 28. Ст. 2895.

© Кравчук С. В.

выступают общественные отношения, обеспечивающие защиту имущественных прав граждан и юридических лиц. Данный вывод обусловлен тем, что ч. 1 ст. 274[3] УК РФ криминализирует незаконное использование телекоммуникационного оборудования, совершенное в целях совершения иного преступления. Подавляющее большинство случаев незаконного использования абонентских терминалов пропуска трафика связано с осуществлением дистанционных мошенничеств, направленных на хищение имущества граждан путем обмана или злоупотребления доверием [5]. Абонентский терминал пропуска трафика выполняет инструментальную функцию в механизме совершения преступлений против собственности, обеспечивая техническую возможность массового воздействия на потенциальных жертв и создания ложного представления о легитимности преступных коммуникаций. Следовательно, хотя незаконное использование телекоммуникационного оборудования само по себе не образует хищения, данное деяние создает непосредственную угрозу имущественным правам граждан и реально способствует совершению преступлений против собственности, что позволяет признавать указанные отношения дополнительным объектом посягательства.

Ст. 23 Конституции Российской Федерации[2] гарантирует каждому право на неприкосновенность частной жизни, право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Использование абонентских терминалов пропуска трафика для осуществления массовых несанкционированных телекоммуникационных рассылок систематически нарушает конституционные права неопределенного круга граждан, вынужденных получать нежелательные коммуникации мошеннического, рекламного или иного характера. Массовый характер таких нарушений создает кумулятивный эффект существенного снижения качества жизни населения и подрыва социального доверия. Однако не во всех случаях незаконное использование телекоммуникационного оборудования непосредственно затрагивает данные права: например, если оборудование используется для совершения единичных целенаправленных мошенничеств без массовых рассылок.

Преступление, предусмотренное ч. 1 ст. 274[3] УК РФ, в том числе считается оконченным при наступлении тяжких последствий как оценочной категории, конкретное содержание которой определяется правоприменителем в каждом конкретном случае с учетом всех обстоятельств дела. В пункте 14 постановления Пленума Верховного Суда Российской Федерации от 15 декабря 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»»[3] дается толкование тяжких последствий, однако оно распространяется только на статьи 272–274[1] УК РФ. Полагаем, что под тяжкими последствиями в статье 274[3] УК РФ следует понимать *причинение значительного имущественного ущерба множеству потерпевших в результате совершенных с использованием оборудования мошенничеств, существенное нарушение работы телекоммуникационной инфраструктуры, создание реальной угрозы общественной безопасности, причинение тяжкого вреда здоровью или смерти по неосторожности вследствие действий, совершенных с использованием оборудования*. Наступление тяжких последствий актуализирует значимость дополнительных объектов преступления, которые в таких случаях реально страдают от преступного посягательства.

Предмет преступления: понятие и признаки

Предмет преступления, предусмотренного ст. 274[3] УК РФ, представляет собой абонентский терминал пропуска трафика или виртуальную телефонную станцию как специализированные технические устройства, воздействуя на которые и используя которые субъект совершает общественно опасное деяние, причиняющее вред охраняемым общественным отношениям. Законодательное определение абонентского терминала пропуска трафика не содержится в диспозиции ст. 274[3] УК РФ, что создает объективные трудности для правоприменительной практики и актуализирует необходимость доктринального толкования данного понятия с учетом технических характеристик оборудования и целей уголовно-правовой охраны. Примечание к ст. 274[3] УК РФ содержит определение понятия «основные части абонентского терминала пропуска трафика», под которыми понимаются технические устройства, включающие в себя радиоэлектронные средства, обеспечивающие возможность приема и (или) передачи коротких текстовых сообщений, телефонных вызовов и (или) сообщений телематических служб в сети подвижной радиотелефонной связи, а также технические устройства, предназначенные для размещения идентификационных модулей абонента.

Системный анализ данного определения позволяет выделить ключевые функциональные признаки абонентского терминала пропуска трафика.

Во-первых, данное устройство обеспечивает возможность приема и передачи различных видов телекоммуникационных сообщений: коротких текстовых сообщений (SMS), телефонных вызовов (голосовой связи), сообщений телематических служб, включая трафик сети Интернет.

[2] Конституция Российской Федерации (принята всенародным голосованием 12 декабря 1993 г.) // Российская газета. 1993, 25 декабря.

[3] Постановление Пленума Верховного Суда Российской Федерации от 15 декабря 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.

© Кравчук С. В.

Во-вторых, устройство предназначено для использования в сети подвижной радиотелефонной связи, то есть в сетях мобильной связи стандартов GSM, UMTS, LTE, 5G, что отличает его от оборудования, работающего исключительно в фиксированных сетях связи или локальных компьютерных сетях.

В-третьих, устройство включает технические средства для размещения множественных идентификационных модулей абонента (SIM-карт), что обеспечивает возможность одновременного использования нескольких абонентских номеров. Именно последний признак представляет критическую особенность, отличающую абонентский терминал пропуска трафика от обычных абонентских устройств, используемых для персональной мобильной связи.

Техническая архитектура типичного абонентского терминала пропуска трафика представляет собой интегрированную программно-аппаратную систему, включающую несколько функциональных компонентов. Центральным элементом выступает так называемый SIM-банк — специализированное устройство, обеспечивающее физическое размещение множественных SIM-карт (от десятков до нескольких сотен) и их программно-управляемую коммутацию. SIM-банк включает корпус с множественными слотами для SIM-карт, контактные группы для электрического соединения, внутреннюю систему коммутации, контроллер управления. Вторым критически важным компонентом являются GSM/LTE-модемы — радиоэлектронные устройства, обеспечивающие физическое подключение к сетям мобильной связи, передачу и прием радиосигналов, реализацию протоколов сотовой связи. В зависимости от производительности терминала используются от единиц до десятков модемов, работающих параллельно для обработки значительных объемов трафика. Третьим компонентом выступает центральный контроллер или процессорный модуль, обеспечивающий координацию работы всех элементов системы, управление коммутацией SIM-карт и модемов, реализацию алгоритмов распределения нагрузки, взаимодействие с внешними системами управления.

Существенным элементом абонентского терминала является специализированное программное обеспечение, реализующее логику управления трафиком, алгоритмы ротации SIM-карт для предотвращения блокировки операторами связи, функции подмены идентификаторов вызывающих абонентов, автоматизированной обработки входящих и исходящих сообщений. Программное обеспечение может быть реализовано как встроенная микропрограмма контроллера либо как отдельный программный комплекс, исполняемый на внешнем компьютере. Вопрос об отнесении программного обеспечения к предмету преступления представляет доктринальную сложность, поскольку традиционное понимание предмета преступления акцентирует материальные объекты. Вместе с тем, современное телекоммуникационное оборудование представляет собой неразрывное единство аппаратных и программных компонентов, и без специализированного программного обеспечения аппаратная платформа не может реализовывать специфические функции абонентского терминала пропуска трафика. Следовательно, программное обеспечение, предназначенное для управления абонентским терминалом, следует рассматривать как составную часть предмета преступления.

Виртуальная телефонная станция как альтернативный предмет преступления представляет собой программно-аппаратный комплекс, реализующий функциональность традиционной телефонной станции программными средствами с использованием технологий передачи голоса по IP-протоколу и интеграции с традиционными сетями телефонной связи через специализированные шлюзы (GSM-шлюзы, SIP-транки). Виртуальная телефонная станция обеспечивает возможность установления, маршрутизации и коммутации телефонных соединений между множественными абонентами, управления вызовами, предоставления дополнительных услуг связи. Ключевой особенностью виртуальной телефонной станции, обусловливающей ее отнесение к предмету преступления, выступает способность обслуживать множественные абонентские номера, осуществлять массовую обработку телефонного трафика, подменять идентификаторы вызывающих абонентов. Виртуальная телефонная станция может быть реализована как на базе специализированных программных платформ (Asterisk, FreeSWITCH), так и с использованием коммерческих решений операторского класса.

Важным для квалификации деяния по ст. 274^3 УК РФ выступает отграничение абонентского терминала пропуска трафика и виртуальной телефонной станции от легального телекоммуникационного оборудования, используемого в правомерных целях. Сами по себе технические возможности оборудования не являются противоправными: аналогичное оборудование может законно использоваться операторами связи для оказания услуг связи на основании лицензии, корпоративными структурами для организации внутренней связи на основании соответствующих разрешений, специализированными организациями для осуществления массовых информационных рассылок с соблюдением требований законодательства. Квалифицирующим признаком, превращающим техническое устройство в предмет преступления, выступает незаконность его использования, определяемая нарушением лицензионных требований, правил применения абонентских номеров, целевым назначением использования оборудования для совершения преступлений.

Следовательно, признание конкретного технического устройства предметом преступления, предусмотренного ст. 274^3 УК РФ, требует комплексной оценки как технических характеристик оборудования, так и обстоятельств его использования.

© Кравчук С. В.

Соотношение объекта и предмета преступления

Методологически корректное разграничение объекта и предмета преступления имеет значение для правильного понимания социально-правовой природы криминализированного деяния и формирования квалификации. Объект преступления как общественные отношения, охраняемые уголовным законом, представляет собой то, на что направлено преступное посягательство, чему причиняется вред в результате совершения преступления. Предмет преступления представляет собой материальный или нематериальный объект, воздействуя на который субъект причиняет вред объекту преступления. Соотношение объекта и предмета носит характер соотношения цели и средства: предмет является тем материальным субстратом, через воздействие на который осуществляется посягательство на охраняемые общественные отношения.

Применительно к преступлению, предусмотренному ст. 274^3 УК РФ, объектом выступают общественные отношения, обеспечивающие установленный порядок функционирования телекоммуникационной инфраструктуры и безопасность компьютерной информации, а предметом — абонентский терминал пропуска трафика или виртуальная телефонная станция. Незаконное использование данного оборудования, представляющего собой предмет преступления, причиняет вред объекту — нарушает установленный порядок использования средств связи, дестабилизирует функционирование телекоммуникационной инфраструктуры, создает угрозу имущественным правам граждан, нарушает конституционные права на неприкосновенность частной жизни. Важно подчеркнуть, что сам абонентский терминал пропуска трафика как материальное устройство не является объектом охраны уголовного закона: ст. 274^3 УК РФ не направлена на защиту данного оборудования от повреждения, уничтожения или хищения. Напротив, целью уголовно-правового запрета выступает предотвращение использования данного оборудования способами, противоречащими установленному правопорядку и создающими угрозу общественной безопасности.

Специфика соотношения объекта и предмета в рассматриваемом составе преступления проявляется в том, что вред объекту причиняется не путем физического уничтожения, повреждения или изменения предмета преступления, а посредством его использования в соответствии с функциональным назначением, но с нарушением установленных правил и в противоправных целях. Данная особенность отличает преступление, предусмотренное ст. 274^3 УК РФ, от других уголовно наказуемых деяний, связанных с уничтожением или повреждением имущества, где вред объекту причиняется через физическое воздействие на предмет. Абонентский терминал пропуска трафика продолжает функционировать в соответствии со своим техническим назначением, однако результаты этого функционирования — массовые телекоммуникационные коммуникации мошеннического или иного противоправного характера — причиняют вред охраняемым общественным отношениям. Следовательно, криминообразующим признаком выступает не факт обладания предметом преступления или воздействия на него, а именно использование предмета определенным образом — незаконно и в противоправных целях.

Заключение

Объект преступления носит сложный многоуровневый характер: родовым объектом выступают общественные отношения в сфере общественной безопасности и общественного порядка; видовым объектом — общественные отношения в сфере безопасности компьютерной информации с расширительным толкованием, охватывающим безопасность функционирования информационно-телекоммуникационной инфраструктуры; основным непосредственным объектом — общественные отношения, обеспечивающие установленный порядок использования средств связи и функционирования телекоммуникационной инфраструктуры; дополнительным объектом — общественные отношения, обеспечивающие защиту имущественных прав граждан.

Предметом преступления выступают абонентский терминал пропуска трафика и виртуальная телефонная станция как специализированные программно-аппаратные комплексы, обеспечивающие возможность одновременного использования множественных абонентских номеров для приема, обработки и передачи телекоммуникационного трафика. Юридически значимыми признаками предмета преступления являются: техническая способность обслуживания множественных абонентских номеров; функциональное назначение для массовой обработки телекоммуникационных сообщений; использование в сетях подвижной радиотелефонной связи или с интеграцией в такие сети. Отграничение предмета преступления от легального оборудования основывается не только на технических характеристиках, но и на характере использования: критерием выступает незаконность использования и направленность на создание условий для совершения преступлений.

Список источников

1. Гирько С. И. Обеспечение общественной безопасности в системе мер защиты личности, общества и государства: состояние, проблемы, перспективы // Административное право и процесс. 2009. № 5. С. 16–19.

2. Кравчук С. В. К вопросу о социальной обусловленности криминализации незаконного использования абонентского терминала пропуска трафика или виртуальной телефонной станции // Проблемы права. 2025. № 4 (100). С. 129–138. DOI: 10.24412/2075-7913-2025-4(100)-129-138

© Кравчук С. В.

3. Кравчук С. В. Технико-правовая характеристика абонентского терминала пропуска трафика и виртуальной телефонной станции как предметов преступления // International Law Journal. 2025. Т. 8, № 8. С. 252–262.

4. Селюков А. С. Преступление против общественной безопасности и общественного порядка // Научный аспект. 2023. Т. 13, № 11. С. 1580–1583.

5. Шульга А. В., Коломоец Д. А. Признаки мошеннических операций, проводимых под видом первичного размещения токенов (ICO) // Вестник Краснодарского университета МВД России. 2018. № 4(42). С. 29–33.

6. Шульга А. В. Уголовно-правовая охрана компьютерной информации // Научно-технологическое обеспечение агропромышленного комплекса России: проблемы и решения: Сборник тезисов по материалам Национальной конференции, Краснодар, 21–22 марта 2018 года / Отв. за выпуск А. Г. Кощаев. Краснодар, 2018. С. 151.

СВЕДЕНИЯ ОБ АВТОРЕ

Кравчук Сергей Владимирович

Соискатель кафедры уголовного права и процесса, Казанский инновационный университет имени В. Г. Тимирясова (ИЭУП) (г. Казань, Россия).
E-mail: 9836565@mail.ru

INFORMATION ABOUT THE AUTHOR

Sergey V. Kravchuk

Postgraduate student in the Department of Criminal Law and Procedure, Kazan Innovative University named after V. G. Timiryasov (IEML) (Kazan, Russia).
E-mail: 9836565@mail.ru

КОНФЛИКТ ИНТЕРЕСОВ

Конфликт интересов отсутствует.

CONFLICT OF INTEREST

There is no conflict of interest.

Дата поступления статьи / Received: 26.05.2026.
Дата рецензирования статьи / Revised: 15.07.2026.
Дата принятия статьи к публикации / Accepted: 20.08.2026.

© Кравчук С. В.