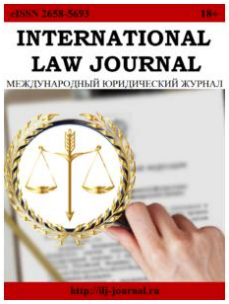
ISSN 2658-5693
https://ilj-journal.ru



Научно-исследовательский журнал «International Law Journal»
https://ilj-journal.ru
2025, Том 8, № 8 / 2025, Vol. 8, Iss. 8 https://ilj-journal.ru/archives/category/publications
Научная статья / Original article
Шифр научной специальности: 5.1.4. Уголовно-правовые науки (юридические науки)
УДК 343.3/.7

Технико-правовая характеристика абонентского терминала пропуска трафика и виртуальной телефонной станции как предметов преступления

[1] Кравчук С.В.,
[1] Казанский инновационный университет имени В.Г. Тимирясова

Аннотация: *в статье проводится комплексное междисциплинарное исследование технико-правовой природы абонентского терминала пропуска трафика и виртуальной телефонной станции как предметов преступления, предусмотренного сатьей 274[3] УК РФ. Автор исследует техническую архитектуру, функциональные характеристики и принципы работы указанного телекоммуникационного оборудования, выявляя криминологически значимые свойства, обусловливающие его использование в преступных целях. Особое внимание уделяется изучению легального определения основных частей абонентского терминала пропуска трафика, содержащегося в примечании к статье, и его соотношению с техническими реалиями функционирования современных телекоммуникационных систем. В работе раскрывается правовая природа предмета преступления и обосновывается специфика предметной характеристики преступлений в сфере информационно-телекоммуникационных технологий. Автором представлен сравнительный обзор легального и нелегального использования телекоммуникационного оборудования, выявлены критерии разграничения правомерного применения технических средств пропуска трафика от их незаконного использования. Исследуются проблемы идентификации и доказывания факта использования абонентских терминалов пропуска трафика в процессе расследования уголовных дел. Сформулированы практические рекомендации по совершенствованию легального определения предмета преступления и унификации терминологии технического и правового характера. Методологическую основу исследования составляет совокупность общенаучных и специальных методов познания, включая системно-структурный, технико-юридический, формально-логический и сравнительно-правовой методы.*

Ключевые слова*: абонентский терминал пропуска трафика, виртуальная телефонная станция, предмет преступления, SIM-банк, GSM-шлюз, телекоммуникационное оборудование, информационная безопасность, уголовная ответственность, идентификационный модуль абонента, технико-правовая характеристика*

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

Поступила в редакцию: 10 сентября 2025 г.; Одобрена после рецензирования: 7 ноября 2025 г.; Принята к публикации: 16 декабря 2025 г.

Technical and legal characteristics of the subscriber terminal for passing traffic and the virtual telephone exchange as objects of crime

[1] Kravchuk S.V.,
[1] **Kazan Innovative University named after V.G. Timiryasov**

Abstract: *the article provides a comprehensive interdisciplinary study of the technical and legal nature of the subscriber traffic terminal and virtual telephone exchange as subjects of a crime provided for by Article 274[3] of the Criminal Code of the Russian Federation. The author examines the technical architecture, functional characteristics and principles of operation of the specified telecommunication equipment, identifying criminologically significant properties that determine its use for criminal purposes. Special attention is paid to the study of the legal definition of the main parts of the subscriber terminal for traffic passage, contained in the note to the article, and its relationship to the technical realities of the functioning of modern telecommunications systems. The paper reveals the legal nature of the subject of the crime and substantiates the specifics of the subject characteristics of crimes in the field of information and telecommunication technologies. The author presents a comparative review of the legal and illegal use of telecommunications equipment, identifies criteria for distinguishing the legitimate use of technical means of traffic transmission from their illegal use. The problems of identification and proof of the fact of using subscriber terminals for passing traffic during the investigation of criminal cases are investigated. Practical recommendations for improving the legal definition of the subject of a crime and the unification of technical and legal terminology are formulated. The methodological basis of the research is a set of general scientific and special methods of cognition, including system-structural, technical-legal, formal-logical and comparative-legal methods.*

Keywords: *subscriber traffic terminal, virtual telephone exchange, crime object, SIM bank, GSM gateway, telecommunication equipment, information security, criminal liability, subscriber identification module, technical and legal characteristics*

For citation: Kravchuk S.V. Technical and legal characteristics of the subscriber terminal for passing traffic and the virtual telephone exchange as objects of crime. International Law Journal. 2025. 8 (8). P. 252 – 262.

The article was submitted: September 10, 2025; Approved after reviewing: November 7, 2025; Accepted for publication: December 16, 2025.

Введение

Трансформация способов совершения преступлений под воздействием научно-технического прогресса представляет собой константную закономерность развития криминальной активности, требующую правового осмысления и законодательного реагирования [13]. Введение в Уголовный кодекс Российской Федерации (далее – УК РФ) [1] статьи 274[3], устанавливающей ответственность за незаконное использование абонентского терминала пропуска трафика или виртуальной телефонной станции, актуализировало проблему научного определения технико-правовой природы предметов данного преступления и выявления их юридически значимых характеристик. Специфика телекоммуникационного оборудования как предмета преступления заключается в необходимости сочетания технического понимания функциональных возможностей устройств с юридическим осмыслением их роли в механизме преступного посягательства.

Абонентский терминал пропуска трафика и виртуальная телефонная станция представляют собой сложные технические комплексы, функционирование которых основано на использовании современных телекоммуникационных технологий и протоколов передачи данных [3]. Криминологическая значимость данного оборудования определяется его способностью обеспечивать массовую передачу телефонных вызовов и сообщений с сокрытием реального источника коммуникации, что создает технические условия для совершения широкого спектра преступлений, прежде всего дистанционных мошенничеств [3]. Вместе с тем, само по себе техническое оборудование данного типа может использоваться и в легитимных целях, что порождает необходимость четкого разграничения правомерного и незаконного применения телекоммуникационных средств на основе объективных технико-правовых критериев.

Научная проблема определения технико-правовой природы предмета преступления, предусмотренного статьей 274[3] УК РФ, обусловлена несколькими взаимосвязанными факторами. Во-первых, законодатель использует специализированную техническую терминологию, содержание которой не всегда очевидно для правоприменителя и требует междисциплинарного исследования с привлечением знаний в области теле-

ISSN 2658-5693
https://ilj-journal.ru

коммуникационных технологий. Во-вторых, примечание к рассматриваемой статье содержит легальное определение основных частей абонентского терминала пропуска трафика, однако степень его полноты и соответствия техническим реалиям нуждается в критическом осмыслении. В-третьих, динамичное развитие телекоммуникационных технологий обусловливает появление новых типов оборудования и способов его использования, что требует выработки гибких подходов к квалификации предмета преступления.

Доктринальная разработанность проблематики предмета преступлений в сфере информационно-телекоммуникационных технологий остается недостаточной, что объясняется относительной новизной соответствующих уголовно-правовых норм и отсутствием устоявшейся судебной практики. Существующие научные исследования преимущественно сосредоточены на изучении традиционных преступлений в сфере компьютерной информации (ст. 272-274 УК РФ), в то время как специфика телекоммуникационного оборудования как предмета преступного посягательства остается малоизученной. Данное обстоятельство актуализирует необходимость комплексного исследования технико-правовых характеристик абонентского терминала пропуска трафика и виртуальной телефонной станции с целью формирования научно обоснованных подходов к их оценке в качестве предметов преступления.

Цель исследования – определение технико-правовой природы абонентского терминала пропуска трафика и виртуальной телефонной станции как предметов преступления, предусмотренного статьей 274^3 УК РФ, и выработка научно обоснованных критериев их правовой оценки.

Для достижения поставленной цели определены следующие **задачи**:

1. Исследовать техническую архитектуру, функциональные характеристики и принципы работы абонентских терминалов пропуска трафика и виртуальных телефонных станций;
2. Изучить легальное определение основных частей абонентского терминала пропуска трафика, содержащееся в примечании к статье, и оценить его соответствие техническим реалиям;
3. Раскрыть правовую природу предмета преступления в сфере телекоммуникаций;
4. Определить критерии разграничения легального и нелегального использования телекоммуникационного оборудования;
5. Выявить проблемы идентификации и доказывания факта использования абонентских терминалов пропуска трафика в правоприменении;
6. Сформулировать рекомендации по совершенствованию законодательного определения предмета преступления и унификации терминологии.

Материалы и методы исследований

Методологическую основу исследования составляет совокупность общенаучных и специально-юридических методов познания, обеспечивающих комплексное междисциплинарное изучение технико-правовой природы предмета преступления, предусмотренного статьей 274^3 УК РФ. Системно-структурный метод применялся для изучения архитектуры абонентских терминалов пропуска трафика и виртуальных телефонных станций, выявления их структурных элементов и функциональных взаимосвязей. Формально-юридический метод использовался для исследования нормативного содержания понятий, закрепленных в рассматрвиаемой статье и примечании к ней, а также для соотношения технико-правовой терминологии уголовного закона и законодательства о связи. Сравнительно-правовой метод позволил выявить особенности регулирования использования телекоммуникационного оборудования в различных отраслях законодательства и провести изучение зарубежных подходов к определению предмета аналогичных преступлений.

Техно-юридический метод, представляющий собой специализированный инструмент исследования правовых норм, регулирующих отношения в сфере информационных технологий, применялся для соотношения технических характеристик телекоммуникационного оборудования и их правового отражения в уголовном законе. Логико-семантический метод использовался для определения содержания легального определения основных частей абонентского терминала пропуска трафика и выявления потенциальных неопределенностей в терминологии законодателя. Метод моделирования позволил реконструировать типичные схемы использования абонентских терминалов пропуска трафика в криминальных целях и определить значимые для квалификации технические параметры оборудования.

Нормативную основу исследования составили: статья 274^3 УК РФ, введенная Федеральным законом от 31 июля 2025 г. № 282-ФЗ [3], Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи» (далее – Федеральный закон «О связи») [2], определяющий правовые основы функционирования телекоммуникационной инфраструктуры, подзаконные нормативные правовые акты, регламентирующие порядок использования средств связи и идентификации абонентов, а также технические регламенты и стандарты в области телекоммуникаций. Эмпирическую базу исследования образовали материалы правоприменения по уголовным делам о преступлениях, совершенных с использованием абонентских терминалов пропуска трафика, экс-

ISSN 2658-5693
https://ilj-journal.ru

пертные заключения компьютерно-технических и телекоммуникационных экспертиз, аналитические материалы операторов связи и уполномоченных государственных органов в сфере регулирования телекоммуникаций.

Техническую основу исследования составила специализированная документация, характеризующая принципы функционирования телекоммуникационного оборудования, включая технические описания GSM-шлюзов, SIM-банков, систем облачной телефонии, протоколы передачи данных в сетях подвижной радиотелефонной связи, стандарты идентификации абонентов и технические требования к оборудованию связи.

Теоретическую основу исследования образовали труды отечественных и зарубежных ученых в области уголовного права, криминологии, информационного права и телекоммуникационных технологий, посвященные проблематике предмета преступления, компьютерных и телекоммуникационных преступлений, а также правового регулирования использования информационных технологий.

Междисциплинарный характер исследования обусловил необходимость интеграции методологических подходов юридической науки и технических дисциплин, что позволило обеспечить понимание как правовой, так и технической составляющих предмета преступления. Критическая оценка существующих научных концепций предмета преступления и их адаптация к специфике телекоммуникационного оборудования позволили выработать оригинальные теоретические подходы к определению технико-правовой природы абонентских терминалов пропуска трафика и виртуальных телефонных станций. Использование комплекса взаимодополняющих методов исследования обеспечило достоверность полученных результатов и их практическую значимость для правоприменительной деятельности.

Результаты и обсуждения

Доктринальное понимание предмета преступления и его специфика в статье 274^3 УК РФ

Предмет преступления традиционно определяется как материальная вещь объективного мира или интеллектуальная ценность, воздействуя на которую либо посредством которой преступник причиняет вред объекту преступления [8, 14]. Предмет преступления не следует смешивать с объектом, поскольку последний представляет собой охраняемые уголовным законом общественные отношения, в то время как предмет образует материальный субстрат, через который осуществляется преступное воздействие на эти отношения [11]. Вместе с тем, предмет преступления не является обязательным признаком состава, присутствуя лишь в тех преступлениях, где законодатель счел необходимым специально указать на материальные или нематериальные объекты, с которыми связано совершение общественно опасного деяния [14].

Применительно к уголовно наказуемым деяниям в сфере информационно-телекоммуникационных технологий категория предмета преступления приобретает особую значимость [5, 15]. Если в имущественных преступлениях предметом выступает вещь материального мира, обладающая стоимостью и потребительскими свойствами, то в компьютерных и телекоммуникационных преступлениях предмет может иметь как материальную природу (техническое устройство), так и нематериальную (компьютерная информация). Статья 274^3 УК РФ предусматривает в качестве предметов преступления абонентский терминал пропуска трафика и виртуальную телефонную станцию, что требует детального исследования правовой природы данных объектов и их соотношение с классическим пониманием предмета преступления.

Абонентский терминал пропуска трафика представляет собой материальный предмет преступления, обладающий вещественной формой и физическими характеристиками, что сближает его с предметами преступлений против собственности. Вместе с тем, криминологическая значимость абонентского терминала пропуска трафика определяется не его стоимостью или иными материальными свойствами, но функциональными возможностями как средства осуществления телекоммуникации в обход установленных правил. Следовательно, предмет преступления, предусмотренный статьей 274^3 УК РФ, характеризуется не столько физическими параметрами, сколько технологическими свойствами и ролью в механизме совершения противоправных действий, что обусловливает необходимость комплексной технико-правовой характеристики данного оборудования.

Виртуальная телефонная станция как предмет преступления обладает еще более специфической природой, поскольку представляет собой программно-аппаратный комплекс, функционирующий на основе технологий облачных вычислений и IP-телефонии [7]. В отличие от абонентского терминала пропуска трафика, имеющего четкую материальную локализацию, виртуальная телефонная станция может не иметь фиксированного физического воплощения, существуя в виде распределенной программной системы, размещенной на удаленных серверах [6]. Данное обстоятельство ставит под вопрос применимость классического понимания предмета преступления как материального объекта и требует расширительного толкования данной категории применительно к цифровым технологиям [10]. Виртуальная телефонная станция образует

ISSN 2658-5693
https://ilj-journal.ru

гибридный предмет преступления, сочетающий материальные элементы (серверное оборудование) и нематериальные компоненты (программное обеспечение, конфигурационные данные).

Законодательное указание на абонентский терминал пропуска трафика и виртуальную телефонную станцию как предметы преступления выполняет несколько правовых функций. Во-первых, оно конкретизирует объективную сторону состава преступления, указывая на специфическое техническое оборудование, незаконное использование которого образует общественно опасное деяние. Во-вторых, законодательное определение предмета преступления ограничивает сферу уголовной ответственности, исключая из неё использование иного телекоммуникационного оборудования, не подпадающего под признаки абонентского терминала пропуска трафика или виртуальной телефонной станции. В-третьих, наличие специфического предмета преступления образует основу для разграничения состава, предусмотренного статьей 274^3 УК РФ, со смежными составами преступлений в сфере компьютерной информации и телекоммуникаций, где предметом выступают иные объекты.

Техническая характеристика абонентского терминала пропуска трафика

Абонентский терминал пропуска трафика представляет собой специализированное телекоммуникационное устройство, предназначенное для автоматизированного приема, обработки и передачи большого объема телефонных вызовов, коротких текстовых сообщений и данных телематических служб в сетях подвижной радиотелефонной связи. Техническая архитектура абонентского терминала пропуска трафика основана на использовании множественных идентификационных модулей абонента (SIM-карт), размещаемых в специализированных устройствах, обеспечивающих их одновременную работу в автоматическом режиме под управлением программного обеспечения. Наиболее распространенными типами абонентских терминалов пропуска трафика являются так называемые SIM-банки и GSM-шлюзы, различающиеся по функциональным возможностям и способам интеграции в телекоммуникационную инфраструктуру.

SIM-банк представляет собой техническое устройство, объединяющее от нескольких десятков до нескольких сотен слотов для размещения SIM-карт, каждая из которых может функционировать как независимый абонентский номер. Конструктивно SIM-банк включает в себя модульную систему размещения идентификационных модулей, контроллер управления, обеспечивающий координацию работы множественных SIM-карт, радиомодули для осуществления связи с базовыми станциями операторов подвижной радиотелефонной связи, блок питания и интерфейсы подключения к управляющему компьютеру или серверу. Программное обеспечение SIM-банка позволяет автоматизировать процессы отправки и приема сообщений, совершения телефонных вызовов, ротации SIM-карт для равномерного распределения нагрузки и минимизации риска блокировки операторами связи.

GSM-шлюз представляет собой более технологически совершенное устройство, обеспечивающее не только пропуск трафика через множественные SIM-карты, но и конвертацию между различными протоколами связи. Типичный GSM-шлюз осуществляет преобразование VoIP-трафика (передача голоса по IP-протоколу) в формат GSM-сигнала, что позволяет направлять телефонные вызовы, поступающие через интернет, в сети подвижной радиотелефонной связи. Техническая функциональность GSM-шлюза включает возможность динамической маршрутизации вызовов через оптимальные каналы связи, автоматической замены неактивных SIM-карт, имитации поведения реальных абонентов для избежания детектирования операторами связи и интеграции с системами автоматического дозвона и рассылки сообщений.

Примечание к статье 274^3 УК РФ содержит легальное определение основных частей 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. Данное определение охватывает ключевые функциональные элементы абонентского терминала пропуска трафика и позволяет идентифицировать как целостные устройства, так и их составные части, что имеет значение для квалификации действий лиц, осуществляющих сборку или модификацию оборудования.

Криминологически значимые технические характеристики абонентского терминала пропуска трафика определяются его способностью обеспечивать массовую коммуникацию с сокрытием реального источника сообщений и вызовов. Использование множественных SIM-карт позволяет распределять криминальный трафик между различными абонентскими номерами, затрудняя выявление противоправной деятельности системами операторов связи. Автоматизация процессов отправки сообщений и совершения вызовов обеспечивает возможность одновременного контакта с тысячами потенциальных жертв мошенничества, что многократно увеличивает общественную опасность использования такого оборудования. Техническая воз-

ISSN 2658-5693
https://ilj-journal.ru

можность дистанционного управления абонентским терминалом пропуска трафика через интернет позволяет лицам осуществлять свою деятельность из любой точки мира, что придает преступлениям трансграничный характер и существенно затрудняет расследование.

Существенным техническим аспектом функционирования абонентского терминала пропуска трафика является механизм взаимодействия с сетями операторов подвижной радиотелефонной связи. Устройство эмулирует поведение обычных абонентских терминалов (мобильных телефонов), регистрируясь в сети оператора и осуществляя обмен сигнализационными сообщениями в соответствии с протоколами GSM/3G/4G. Однако в отличие от легитимного использования, абонентский терминал пропуска трафика характеризуется аномальными шаблонами активности: чрезмерно высоким количеством исходящих вызовов или сообщений, отсутствием входящих вызовов, нетипичной географической локализацией при большом количестве обслуживаемых номеров, специфическими временными шаблонами активности. Эти технические индикаторы используются операторами связи для выявления незаконного оборудования и правоохранительными органами для доказывания факта использования абонентского терминала пропуска трафика.

Техническая характеристика виртуальной телефонной станции

Виртуальная телефонная станция представляет собой программно-аппаратный комплекс, реализующий функциональность традиционной офисной автоматической телефонной станции на базе технологий IP-телефонии и облачных вычислений. В отличие от физической телефонной станции, требующей установки специализированного оборудования в помещении пользователя, виртуальная телефонная станция функционирует как распределенная программная система, размещенная на серверах провайдера услуг и доступная пользователям через интернет-соединение. Техническая архитектура виртуальной телефонной станции основана на протоколе SIP (Session Initiation Protocol) и кодеках передачи голоса, обеспечивающих преобразование аналогового звука в цифровые пакеты данных для передачи по IP-сетям.

Функциональные возможности виртуальной телефонной станции включают создание множественных внутренних номеров, автоматическую маршрутизацию входящих и исходящих вызовов, переадресацию звонков, организацию конференц-связи, интеграцию с системами управления взаимоотношениями с клиентами, запись разговоров и детальную аналитику телефонного трафика. В легитимном использовании виртуальная телефонная станция обеспечивает организациям и индивидуальным предпринимателям доступ к профессиональным телекоммуникационным сервисам без необходимости инвестиций в дорогостоящее оборудование и его техническое обслуживание. Программная природа виртуальной телефонной станции обеспечивает высокую гибкость конфигурации, масштабируемость и возможность быстрого развертывания.

Криминальное использование виртуальной телефонной станции основано на эксплуатации её технических возможностей для совершения мошенничеств и иных преступлений с сокрытием реальной идентичности звонящего. Виртуальная телефонная станция позволяет подменять определитель номера (Caller ID spoofing), отображая на телефоне жертвы произвольный телефонный номер, в том числе номера государственных органов, банков или иных доверенных организаций. Данная техническая возможность широко используется в схемах социальной инженерии, когда преступники представляются сотрудниками правоохранительных органов или финансовых учреждений для получения конфиденциальной информации или склонения жертвы к переводу денежных средств. Автоматизация процесса совершения вызовов через виртуальную телефонную станцию обеспечивает возможность массовых мошеннических контактов с одновременным использованием скриптов обмана и голосовых роботов.

Техническая специфика виртуальной телефонной станции как предмета преступления заключается в её распределенном характере и отсутствии единого физического воплощения. Функционирование виртуальной телефонной станции обеспечивается совокупностью программных компонентов (серверное ПО, системы управления вызовами, базы данных конфигурации), аппаратных ресурсов (серверы, системы хранения данных, сетевое оборудование) и телекоммуникационных каналов (подключение к операторам телефонной связи через SIP-транки или GSM-шлюзы). При этом различные элементы виртуальной телефонной станции могут быть территориально распределены и размещены на серверах, находящихся в различных юрисдикциях, что создает существенные сложности для идентификации предмета преступления и его процессуального изъятия.

Существенным аспектом технической характеристики виртуальной телефонной станции является механизм её подключения к традиционным телефонным сетям. Для обеспечения возможности совершения вызовов на обычные телефонные номера виртуальная телефонная станция должна быть интегрирована с услугами операторов телефонной связи через специализированных провайдеров VoIP-телефонии. Легитимные провайдеры осуществляют идентификацию клиентов и контроль за характером использования услуг в со-

ISSN 2658-5693
https://ilj-journal.ru

ответствии с требованиями законодательства о связи. Однако существование нелегальных провайдеров VoIP-услуг, не осуществляющих надлежащий контроль и предоставляющих возможность подмены номеров и анонимного использования, создает техническую основу для криминального применения виртуальных телефонных станций. Выявление факта использования виртуальной телефонной станции в противоправных целях требует технического анализа маршрутизации вызовов, изучения логов серверного оборудования и исследования конфигурации программного обеспечения.

Критерии разграничения легального и нелегального использования телекоммуникационного оборудования

Абонентские терминалы пропуска трафика и виртуальные телефонные станции как технические средства не являются изначально противоправными и могут использоваться в легитимных целях при соблюдении установленных правил функционирования сетей связи. Следовательно, криминализация незаконного использования такого оборудования предполагает наличие объективных критериев разграничения правомерного и неправомерного применения телекоммуникационных средств. Выработка таких критериев представляет собой актуальную научно-практическую задачу, решение которой необходимо для обеспечения единообразного правоприменения и защиты прав добросовестных пользователей телекоммуникационного оборудования.

Первым и основополагающим критерием разграничения легального и нелегального использования телекоммуникационного оборудования является соответствие деятельности требованиям законодательства о связи и лицензионным условиям. Статья 29 Федерального закона «О связи» [2] устанавливает требование обязательной регистрации радиоэлектронных средств и высокочастотных устройств, к числу которых относятся компоненты абонентских терминалов пропуска трафика. Эксплуатация незарегистрированного оборудования, способного создавать помехи функционированию сетей связи или нарушать установленный порядок использования радиочастотного спектра, образует административное правонарушение, а при наличии дополнительных квалифицирующих признаков может влечь уголовную ответственность по статье 274^3 УК РФ.

Вторым критерием является соблюдение правил идентификации абонентов и конечного оборудования. Постановление Правительства Российской Федерации от 30 декабря 2024 г. № 1994 «Об утверждении Правил оказания услуг телефонной связи и перечня организаций, имеющих право осуществлять подтверждение сведений об абоненте - физическом лице» [4] устанавливает обязанность операторов связи осуществлять идентификацию абонентов при заключении договоров на оказание услуг связи. Использование множественных SIM-карт, приобретенных с нарушением правил идентификации (так называемых «серых» SIM-карт), или оформленных на подставных лиц, образует существенный индикатор незаконности использования абонентского терминала пропуска трафика. Массовое использование SIM-карт, зарегистрированных на лиц, не имеющих реального отношения к их эксплуатации, свидетельствует о намерении скрыть реального пользователя оборудования, что характерно для криминального применения.

Третьим критерием выступает характер и объем передаваемого трафика. Легитимное использование многоканального телекоммуникационного оборудования предприятиями и организациями характеризуется сбалансированным соотношением входящих и исходящих вызовов, наличием типичных форм деловой коммуникации, территориальной привязкой к месту нахождения юридического лица. В противоположность этому, криминальное использование абонентского терминала пропуска трафика проявляется в аномально высоком объеме исходящего трафика при минимальном количестве входящих вызовов, массовых рассылках однотипных сообщений, использовании сценариев автоматизированного обзвона. Операторы связи применяют системы автоматического мониторинга, выявляющие подобные аномалии и классифицирующие трафик как потенциально незаконный.

Четвертым критерием является цель использования оборудования, которая в силу прямого указания части первой статьи 274^3 УК РФ образует обязательный признак состава преступления. Совершение деяния в целях совершения иного преступления свидетельствует о заведомой противоправности использования телекоммуникационного оборудования и исключает возможность квалификации такого использования как добросовестного заблуждения или технической ошибки. Установление цели совершения иного преступления требует изучения всей совокупности объективных и субъективных обстоятельств дела, включая содержание передаваемых сообщений, характер совершаемых вызовов, наличие фактов причинения имущественного вреда гражданам и организациям, показания лиц, получивших мошеннические звонки или сообщения.

Пятым критерием выступает профессиональный или систематический характер деятельности по эксплуатации телекоммуникационного оборудования. Единичное использование виртуальной телефонной стан-

ISSN 2658-5693
https://ilj-journal.ru

ции для осуществления корпоративной связи в рамках легальной предпринимательской деятельности качественно отличается от систематической эксплуатации множественных абонентских терминалов пропуска трафика в целях предоставления услуг по незаконному пропуску криминального трафика иным лицам. Формирование устойчивой криминальной инфраструктуры, включающей техническую поддержку, аренду каналов связи, привлечение подставных лиц для регистрации SIM-карт, свидетельствует о профессиональном характере противоправной деятельности и повышенной общественной опасности деяния.

Проблемы идентификации и доказывания факта использования абонентских терминалов пропуска трафика

Процесс расследования преступлений, предусмотренных статьей 274^3 УК РФ, сопряжен с рядом специфических проблем технического и процессуального характера, обусловленных особенностями телекоммуникационного оборудования [9] как предмета преступления. Первостепенной задачей расследования является идентификация технического устройства в качестве абонентского терминала пропуска трафика или виртуальной телефонной станции, что требует специальных технических знаний и применения экспертных методов исследования [12]. Внешне абонентский терминал пропуска трафика может не иметь очевидных отличительных признаков, представляя собой компактное устройство с множеством слотов для SIM-карт, которое может быть ошибочно принято за легальное оборудование связи.

Осмотр места происшествия при обнаружении абонентского терминала пропуска трафика должен осуществляться с участием специалиста, обладающего компетенциями в области телекоммуникационных технологий. Специалист обеспечивает правильную фиксацию технических характеристик оборудования, схемы его подключения к сетям связи и электропитанию, наличия управляющих компьютеров и программного обеспечения, количества установленных SIM-карт и их идентификационных данных. Существенное значение для последующего доказывания имеет фиксация состояния оборудования на момент обнаружения: наличия активных соединений с сетью оператора, выполняемых в момент осмотра операций по отправке сообщений или совершению вызовов, содержимого оперативной памяти устройств и логов программного обеспечения.

Назначение компьютерно-технической и телекоммуникационной экспертиз является обязательным элементом доказывания по делам о преступлениях, предусмотренных статьей 274^3 УК РФ. На разрешение экспертов ставятся вопросы о функциональном назначении изъятого оборудования, его соответствии признакам абонентского терминала пропуска трафика, установленным примечанием к статье 274^3 УК РФ, о техническом состоянии устройства и его работоспособности, о количестве обслуживаемых SIM-карт и их принадлежности конкретным операторам связи. Особое значение имеет исследование программного обеспечения, управляющего работой оборудования, с целью установления его функциональных возможностей, анализа логов использования и выявления следов совершения конкретных противоправных действий.

Взаимодействие с операторами связи образует важный элемент доказывания по делам о незаконном использовании телекоммуникационного оборудования. Операторы связи обладают технической информацией о характере трафика, проходившего через идентификационные модули, установленные в абонентском терминале пропуска трафика, о географической локализации устройства на основании данных базовых станций, о фактах блокировки номеров в связи с выявлением подозрительной активности. Получение детализации соединений (CDR – Call Detail Records) позволяет установить конкретные факты совершения вызовов и отправки сообщений, идентифицировать потерпевших и определить масштаб причиненного вреда. Анализ маршрутизации трафика может выявить использование транзитных операторов и международных каналов связи, что свидетельствует о сложности криминальной схемы.

Доказывание факта использования виртуальной телефонной станции представляет еще большую сложность в силу её распределенной программной природы. Традиционные следственные действия, такие как осмотр места происшествия и выемка, могут не привести к обнаружению физических компонентов виртуальной телефонной станции, если её функционирование обеспечивается облачными сервисами, размещенными на удаленных серверах. В таких случаях доказывание требует получения информации от провайдеров VoIP-услуг, анализа сетевого трафика, исследования конфигурационных файлов и учетных записей пользователей. При трансграничном характере использования виртуальной телефонной станции возникает необходимость международного правового сотрудничества для получения доказательств, что существенно удлиняет сроки расследования.

Существенной проблемой доказывания является установление субъективной стороны преступления, в частности цели совершения иного преступления или осознания неизбежности наступления тяжких последствий. Факт обнаружения абонентского терминала пропуска трафика не свидетельствует о наличии умысла на его использование в преступных целях. Необходимо доказать, что лицо осознавало незаконный характер

ISSN 2658-5693
https://ilj-journal.ru

использования оборудования и предвидело возможность или неизбежность совершения с его помощью иных преступлений либо причинения существенного вреда. Это требует комплексного исследования объективных обстоятельств дела: содержания сообщений и характера вызовов, наличия фактов мошенничества с использованием данного оборудования, конспиративного характера размещения устройств, использования подставных лиц для регистрации SIM-карт и иных обстоятельств, свидетельствующих о противоправной деятельности.

Выводы

Предмет преступления в виде абонентского терминала пропуска трафика или виртуальной телефонной станции обладает специфической технико-правовой природой, сочетающей материальные характеристики технического оборудования и функциональные свойства средства осуществления телекоммуникации. Криминологическая значимость данного предмета определяется не физическими параметрами оборудования, но его технологическими возможностями обеспечения массовой коммуникации с сокрытием реального источника сообщений и вызовов, что создает инструментальную основу для совершения широкого спектра преступлений.

Абонентский терминал пропуска трафика представляет собой материальный предмет преступления, имеющий физическое воплощение в виде технического устройства, объединяющего множественные идентификационные модули абонента и радиоэлектронные средства для осуществления связи в сетях подвижной радиотелефонной связи. Легальное определение основных частей абонентского терминала пропуска трафика, содержащееся в примечании к исследуемой статье, соответствует технической реальности и охватывает ключевые функциональные элементы устройства, обеспечивая возможность идентификации предмета преступления в правоприменении.

Виртуальная телефонная станция образует специфический гибридный предмет преступления, сочетающий материальные компоненты (серверное оборудование) и нематериальные элементы (программное обеспечение), что обусловливает необходимость расширительного толкования классического понимания предмета преступления. Распределенная программная природа виртуальной телефонной станции создает существенные сложности для её процессуальной фиксации и изъятия, требуя разработки специализированных методов доказывания.

Разграничение легального и нелегального использования телекоммуникационного оборудования основывается на совокупности критериев: соответствии требованиям законодательства о связи, соблюдении правил идентификации абонентов, характере и объеме передаваемого трафика, цели использования оборудования и систематичности противоправной деятельности. Ни один из указанных критериев не является достаточным сам по себе, но их совокупная оценка позволяет установить противоправный характер использования телекоммуникационных средств.

Процесс идентификации и доказывания факта использования абонентских терминалов пропуска трафика и виртуальных телефонных станций сопряжен со значительными техническими и процессуальными сложностями, обусловленными спецификой телекоммуникационного оборудования. Эффективное расследование преступлений, предусмотренных статьей 274^3 УК РФ, требует обязательного участия специалистов и экспертов, обладающих компетенциями в области телекоммуникационных технологий, тесного взаимодействия с операторами связи и уполномоченными государственными органами, а также применения современных методов цифровой криминалистики.

Совершенствование правового регулирования и правоприменения в рассматриваемой сфере требует унификации технико-правовой терминологии, разработки методических рекомендаций по выявлению и расследованию преступлений, предусмотренных статьей 274^3 УК РФ, формирования специализированных компетенций следователей и судей в области телекоммуникационных технологий. Имеется потребность в разъяснениях Пленума Верховного Суда Российской Федерации по вопросам квалификации преступлений, связанных с незаконным использованием телекоммуникационного оборудования, и определяющего единообразные подходы к толкованию признаков предмета преступления.

Список источников

1. Уголовный кодекс Российской Федерации // Собрание законодательства Российской Федерации. 1996, № 25, Ст. 2954.

2. Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи» // Российская газета, 10 июля 2003 г.

3. Федеральный закон от 31 июля 2025 г. № 282-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» // Российская газета, 6 августа 2025 г.

4. Постановление Правительства Российской Федерации от 30 декабря 2024 г. № 1994 «Об утверждении Правил оказания услуг телефонной связи и перечня организаций, имеющих право осуществлять подтверждение сведений об абоненте – физическом лице» // Собрание законодательства Российской Федерации. 2025. № 1. С. 42.

5. Бегишев И.Р., Бикеев И.И. Преступления в сфере обращения цифровой информации. Казань: Изд-во «Познание» Казанского инновационного университета, 2020. 300 с. (Серия «Цифровая безопасность»).

6. Буряков В.М. Виртуальные базовые станции сотовой связи в контексте информационной безопасности России // Наукоемкие технологии в космических исследованиях Земли. 2023. Т. 15. № 6. С. 43 – 51. doi:10.36724/2409-5419-2023-15-6-43-51

7. Дронова О.Б., Проваторова К.В., Сапухин А.А. Интернет-ресурсы, используемые в процессе информационного обеспечения раскрытия и расследования мошенничеств, совершенных с использованием средств мобильной связи и сети Интернет // Вестник волгоградской академии мвд россии. 2021. № 3 (58). С. 137 – 144.

8. Евтушенко И.И. Понятие и место предмета преступления в конструкции состава преступления // Ученые записки Крымского федерального университета имени В.И. Вернадского. Юридические науки. 2023. Т. 9. № 1. С. 326 – 333.

9. Климов Д.А. Особенности эксплуатации современного телекоммуникационного оборудования // T-Comm – Телекоммуникации и Транспорт. 2012. № 8. С. 26 – 27.

10. Козаев Н.Ш. Киберпреступность в современном мире: тенденции, вызовы и стратегии противодействия // Гуманитарные, социально-экономические и общественные науки. 2024. № 11. С. 146 – 153. doi:10.24412/2220-2404-2024-11-9

11. Коргулев А.Г. Соотношение предмета и объекта преступления // Гуманитарные, социально-экономические и общественные науки. 2020. № 7. С. 127 – 131.

12. Машекуашева М.Х. Некоторые особенности личности преступника, совершающего мошенничество с использованием телекоммуникационного и компьютерного оборудования // Право и управление. 2023. № 11. С. 504 – 507.

13.Русскевич Е.А. Уголовно-правовое противодействие преступлениям, совершаемым с использованием информационно-коммуникационных технологий: учеб. пособие. М.: ИНФРА- М, 2018. 115 с. (Высшее образование: Магистратура).

14. Гришко А.Я., Антонян Е.А., Беляков А.Ю. и др. Уголовное право Российской Федерации. Общая часть: учебник. Москва: Общество с ограниченной ответственностью «Научно-издательский центр ИНФРА-М», 2025. 557 с. ISBN 978-5-16-018447-0. DOI 10.12737/2007669

15. Шутова А.А. Конструкция как конструктивный признак отдельных составов электричества // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2015. № 2 (30). С. 201 – 205.

References

1. Criminal Code of the Russian Federation. Collected Legislation of the Russian Federation. 1996, No. 25, Article 2954.

2. Federal Law of July 7, 2003 No. 126-FZ "On Communications". Rossiyskaya Gazeta, July 10, 2003.

3. Federal Law of July 31, 2025 No. 282-FZ "On Amendments to Certain Legislative Acts of the Russian Federation". Rossiyskaya Gazeta, August 6, 2025.

4. Resolution of the Government of the Russian Federation of December 30, 2024 No. 1994 "On Approval of the Rules for the Provision of Telephone Communication Services and the List of Organizations Authorized to Confirm Information about an Individual Subscriber". Collected Legislation of the Russian Federation. 2025. No. 1. P. 42.

5. Begishev I.R., Bikeev I.I. Crimes in the Sphere of Digital Information Circulation. Kazan: Poznanie Publishing House of Kazan Innovation University, 2020. 300 p. (Digital Security Series).

6. Buryakov V.M. Virtual Base Stations of Cellular Communications in the Context of Russia's Information Security. High-Technologies in Space Research of the Earth. 2023. Vol. 15. No. 6. P. 43 – 51. doi:10.36724/2409-5419-2023-15-6-43-51

7. Dronova O.B., Provatorova K.V., Sapukhin A.A. Internet Resources Used in the Process of Information Support for the Detection and Investigation of Frauds Committed Using Mobile Communications and the Internet. Bulletin of the Volgograd Academy of the Ministry of Internal Affairs of Russia. 2021. No. 3 (58). P. 137 – 144.

8. Yevtushenko I.I. Concept and Place of the Subject of a Crime in the Construction of a Crime's Composition. Scientific Notes of the Crimean Federal University named after V.I. Vernadsky. Legal Sciences. 2023. Vol. 9. No. 1. P. 326 – 333.

9. Klimov D.A. Features of Operation of Modern Telecommunications Equipment. T-Comm – Telecommunications and Transport. 2012. No. 8. P. 26 – 27.

10. Kozayev N.Sh. Cybercrime in the Modern World: Trends, Challenges, and Counteraction Strategies. Humanitarian, Socio-Economic, and Social Sciences. 2024. No. 11. P. 146 – 153. doi:10.24412/2220-2404-2024-11-9

11. Korgulev A.G. The Correlation of the Subject and Object of a Crime. Humanitarian, Socio-Economic and Social Sciences. 2020. No. 7. P. 127 – 131.

12. Mashekuasheva M.Kh. Some Personality Traits of a Criminal Committing Fraud Using Telecommunications and Computer Equipment. Law and Management. 2023. No. 11. P. 504 – 507.

13. Russkevich E.A. Criminal-Legal Counteraction to Crimes Committed Using Information and Communication Technologies: A Textbook. Moscow: INFRA-M, 2018. 115 p. (Higher education: Master's degree).

14. Grishko A.Ya., Antonyan E.A., Belyakov A.Yu. et al. Criminal Law of the Russian Federation. General Part: Textbook. Moscow: Limited Liability Company "Scientific Publishing Center INFRA-M", 2025. 557 p. ISBN 978-5-16-018447-0. DOI 10.12737/2007669

15. Shutova A.A. Design as a Structural Feature of Individual Electrical Compositions. Legal Science and Practice: Bulletin of the Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia. 2015. No. 2 (30). P. 201 – 205.

Информация об авторе

Кравчук С.В., соискатель кафедры уголовного права и процесса, Казанский инновационный университет имени В.Г. Тимирясова