

УГОЛОВНОЕ ПРАВО И ОСОБЕННОСТИ КВАЛИФИКАЦИИ ПРЕСТУПЛЕНИЙ

Виктор Николаевич БОРКОВ

доктор юридических наук, профессор
Омская академия МВД России (г. Омск)
начальник кафедры уголовного права
borkov_viktor@bk.ru

Научная статья
УДК 343.34:004

ОСОБЕННОСТИ И ПРАВИЛА КВАЛИФИКАЦИИ НЕЗАКОННОГО ИСПОЛЬЗОВАНИЯ АБОНЕНТСКОГО ТЕРМИНАЛА ПРОПУСКА ТРАФИКА

КЛЮЧЕВЫЕ СЛОВА. Использование абонентского терминала, обслуживание абонентского терминала, цель совершения преступления, соучастие в преступлении, создание условий для преступления, прикосновенность к преступлению.

АННОТАЦИЯ. *Введение.* Незаконное использование абонентского терминала пропуска трафика позволяет преступникам действовать анонимно, в больших масштабах и удаленно, что значительно повышает общественную опасность хищений, склонения к участию в диверсиях и террористических актах. Само по себе обеспечение функционирования SIM-бокса, хотя и создает условия для преступлений, не считалось до недавнего времени соучастием в их совершении. Данный пробел криминализации был устранен путем дополнения Уголовного кодекса Российской Федерации статьей 274.3. **Методы.** Исследование, результаты которого представлены в статье, опиралось на диалектический метод познания. В ходе работы применялись логический и системно-структурный методы, а также анализ, синтез, индукция и дедукция. **Результаты.** Установлено, что в ч. 1 ст. 274.3 УК РФ речь идет о трех альтернативных преступных посягательствах: использование при совершении преступления абонентского терминала пропуска трафика, обслуживаемого другим лицом; обслуживание абонентского терминала для совершения преступлений другими лицами; использование абонентского терминала для совершения преступления лицом, которое само обеспечивает функционирование данного терминала. Показано, что «цель совершения иного преступления» при квалификации действий субъекта, только обеспечивающего функционирование терминала, должна толковаться расширительно: необходимо учитывать осознание виновным создания им условий для преступной деятельности других лиц. Иное представление лишило бы рассматриваемую норму ее основного предназначения – криминализации создания условий для совершения других посягательств с использованием информационно-телекоммуникационных технологий при отсутствии признаков соучастия. Предложены критерии определения тяжких последствий незаконного использования или обслуживания абонентского терминала (ч. 1 ст. 274.3 УК РФ). О наличии таковых, в частности, могут свидетельствовать масштабы преступной деятельности, количество совершённых с использованием терминала посягательств и пострадавших, а также вред, причиненный безопасности общества и государства. Тяжкими последствиями использования терминала или виртуальной телефонной станции является создание условий для совершения террористического акта, диверсии, посягательства на жизнь государственного деятеля.

ВВЕДЕНИЕ

Стремительная цифровизация общественных отношений, внедрение передовых телекоммуникационных технологий и рост доступности специализированного программного обеспечения создали принципиально новые условия для совершения противоправных деяний. На смену традиционным, преимущественно контактными формам преступного поведения приходят дистанционные, высокотехнологичные и хорошо замаскированные посягательства. В этих условиях особую общественную опасность представляет использование преступниками абонентских терминалов пропуска трафика и виртуальных телефонных станций. Данные инструменты позволяют действовать анонимно, в неограниченных масштабах и из любой точки мира, что кардинально трансформирует механизмы совершения таких тяжких преступлений, как хищения, склонение к диверсионной деятельности и терроризму.

Актуальность исследования, результаты которого представлены в настоящей статье, обусловлена рядом факторов. Во-первых, современное состояние преступности характеризуется динамичностью и высокой адаптивностью: как справедливо отмечается в научной литературе, «схемы совершения цифровых посягательств постоянно изменяются, они эволюционируют с опережением законодательного реагирования» [1, с. 27]. Это создает ситуацию перманентного отставания правовых механизмов от криминальных инноваций, что требует постоянного переосмысления подходов к противодействию [2]. Во-вторых, вплоть до недавнего времени в уголовном законодательстве существовал значительный пробел. Ранее упоминавшиеся в трудах ученых «базовые приемы обмана», такие как «подмена телефонного номера» [3, с. 211; 4, с. 13], не имели самостоятельной квалификации в случаях, когда лицо лишь создавало технические условия для неопределенной по времени и месту преступной деятельности других лиц. В этих случаях действия операторов технических систем зачастую было невозможно признать соучастием в классическом понимании, что позволяло пособникам избегать ответственности. В-третьих, введение в Уголовный кодекс Российской Федерации (далее – УК РФ) ст. 274.3 стало значимым шагом на пути к устранению описанного пробела. Однако практика применения данной нормы сталкивается со сложностями ее толкования. Часть 1 ст. 274.3 УК РФ ставит наступление ответственности за незаконное использование абонентского терминала пропуска трафика, виртуальной телефонной станции или обеспечение их функционирования в зависимости от цели совершения «иного преступления» либо наступления тяжких последствий. Особого внимания заслуживает субъективная сторона деяния: по смыслу закона, норма распространяется не только на лиц, обеспечивающих функционирование абонентского терминала или виртуальной телефонной станции для «совершения иного преступления», но и на самих исполнителей, которые осознают, что их противоправные действия (звонки, призывы)

технически обеспечиваются посредством указанного оборудования.

Целью нашего исследования было выявление специфики объективных и субъективных признаков составов преступлений, предусмотренных ст. 274.3 УК РФ, определение границ их применения и выработка предложений по совершенствованию правоприменительной практики в условиях ускоряющейся эволюции цифровых угроз.

МЕТОДЫ

Методологическую основу исследования составил всеобщий диалектический метод познания. С его помощью изучались влияющие друг на друга и порождающие друг друга изменяющиеся способы совершения посягательств на личность, собственность, общество, государство и развивающиеся информационно-телекоммуникационные технологии. В качестве основного критерия истинности толкования вносимых в уголовный закон изменений определена их обусловленность модификацией приемов преступной деятельности.

Анализ основного и квалифицированных составов преступлений, предусмотренных в ст. 274.3 УК РФ, позволил выявить основные альтернативные посягательства, квалифицируемые по данной норме, уточнить их способы совершения и субъектный состав. Установлено соотношение цели совершения иного преступления и тяжких последствий как признаков основного состава, даны рекомендации по квалификации совершения рассматриваемого посягательства организованной группой.

Обращение к методу синтеза создало предпосылки к формированию целостного представления о составах преступлений, предусмотренных ст. 274.3 УК РФ, предполагающего соответствие их объективных признаков субъективным и наоборот. Подобный подход позволил изучить связь между консолидированным содержанием признаков состава преступления и его общественной опасностью.

Логический метод был востребован при исследовании сущности и содержания незаконного использования абонентского терминала пропуска трафика, виртуальной телефонной станции в целях совершения иного преступления или с тяжкими последствиями. Применение данного метода позволило раскрыть объективную связь между количеством «измененных» звонков и пострадавших, то есть масштабами преступной деятельности и мерой вреда, причиненного безопасности общества и государства.

Системно-структурный метод применялся для определения места незаконного использования абонентского терминала пропуска трафика или виртуальной телефонной станции в системе уголовно-правовой охраны общественных отношений, формулирования правил квалификации рассматриваемого преступления по совокупности с посягательствами на собственность, общественную безопасность и безопасность государства.

РЕЗУЛЬТАТЫ

Установление обозначенной в ч. 1 ст. 274.3 УК РФ «цели совершения иного преступления» «требует изучения всей совокупности объективных и

Viktor N. BORKOV

Doctor of Law, Professor

Omsk Academy of the Ministry of the Interior of Russia (Omsk, Russia)

Head of the Department of Criminal Law

borkov_viktor@bk.ru

FEATURES AND RULES FOR QUALIFYING THE ILLEGAL USE OF A SUBSCRIBER TERMINAL FOR TRANSMITTING TRAFFIC**KEYWORDS.** Use of a subscriber terminal, maintenance of a subscriber terminal, purpose of committing a crime, complicity in a crime, creation of conditions for a crime, involvement in a crime.

ANNOTATION. Introduction. Illegal use of a subscriber terminal for transmitting traffic allows criminals to act anonymously, on a large scale and remotely, which significantly increases the public danger of theft, incitement to participate in sabotage and terrorist acts. The mere operation of a SIM box, although it creates the conditions for crimes, was not considered complicity in their commission until recently. This gap in criminalization was eliminated by supplementing the Criminal Code of the Russian Federation with Art. 274.3. **Methods.** The study, the results of which are presented in the article, was based on the dialectical method of cognition. In the course of the work, logical and system-structural methods, as well as analysis, synthesis, induction and deduction were used. **Results.** It was established that part 1 of Art. 274.3 of the Criminal Code of the Russian Federation refers to three alternative criminal offenses: use in committing a crime of a subscriber terminal for transmitting traffic, serviced by another person; servicing a subscriber terminal for committing crimes by other persons; the use of a subscriber terminal to commit a crime by a person who ensures the operation of the terminal. It is shown that the «intent to commit another crime» when qualifying the actions of a subject solely ensuring the operation of the terminal should be interpreted broadly: it is necessary to take into account the perpetrator's awareness of creating conditions conducive to the criminal activity of others. Any other interpretation would deprive the norm in question of its primary purpose – criminalizing the creation of conditions conducive to the commission of other offenses using information and telecommunications technologies in the absence of evidence of complicity. Criteria for determining the grave consequences of the illegal use or maintenance of a subscriber terminal (part 1 of Art. 274.3 of the Criminal Code of the Russian Federation) are proposed. The presence of such consequences may be evidenced, in particular, by the scale of the criminal activity, the number of offenses committed using the terminal and the number of victims, as well as the harm caused to the security of society and the state. Grave consequences of using a terminal or virtual telephone exchange include creating conditions conducive to committing an act of terrorism, sabotage, or an attempt on the life of a public figure.

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» [5, с. 258]. В уголовном законе указание на «цель совершения преступления» используется, например, применительно к организации незаконной миграции (п. «в» ч. 2 ст. 322.1 УК РФ). Согласно разъяснениям высшей судебной инстанции, такое посягательство может быть совершено как самим лицом, организующим незаконную миграцию, «в отношении иностранных граждан или лиц без гражданства», так и мигрантами. «Если лицо, организовавшее незаконную миграцию ... приняло участие в совершении указанного преступления, его сокрытии или облегчении совершения, то его действия при наличии оснований квалифицируются по совокупности преступлений, предусмотренных пунктом «в» части 2 или частью 3 статьи 322.1 УК РФ и со-

ответствующей статьей (пунктом, частью статьи) Особенной части Уголовного кодекса Российской Федерации, со ссылкой в необходимых случаях на часть 3 или часть 5 статьи 33 УК РФ»¹. Также по совокупности преступлений квалифицируются действия лица, которое совершает предусмотренное законом посягательство в сфере компьютерной информации для облегчения совершения или других преступлений².

Демонстрируемый Верховным Судом Российской Федерации подход позволяет утверждать, что преступление, предусмотренное ч. 1 ст. 274.3 УК РФ, может состоять в обеспечении субъектом функционирования абонентского терминала для совершения преступлений как им самим, так и другими лицами. «Цель совершения иного преступления» в первом приближении предполагает осознание не только того, что абонентский терминал позволит облегчить или скрыть любое общественно опасное посягательство, но и конкретного его вида. В таком случае лицо, обеспечивающее

¹ См. п. 10 Постановления Пленума Верховного Суда Российской Федерации от 09.07.2020 № 18 «О судебной практике по делам о незаконном пересечении Государственной границы Российской Федерации и преступлениях, связанных с незаконной миграцией» (ред. от 23.12.2025).

² См. п. 16 Постановления Пленума Верховного Суда Российской Федерации от 15.12.2022 № 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».

функционирование абонентского терминала с указанной целью, могло бы быть признано исполнителем преступления, предусмотренного ст. 274.3 УК РФ, только в том случае, если оно одновременно выступало бы соучастником мошенничества, финансирования экстремистской деятельности, террористического акта, диверсии или других преступлений.

Понятно, что организатор и пособник всегда осведомлены о том, в каком конкретно посягательстве они участвуют, причем еще до его совершения. Для реализации заложенной в смысл ст. 274.3 УК РФ идеи законодателя следовало бы сформулировать норму иначе: установить ответственность за само по себе незаконное обеспечение функционирования абонентского терминала, а то есть применить конструкцию состава опасности и подвергнуть криминализации создание угрозы содействия совершению неопределенного круга противоправных деяний. Например, ст. 187 УК РФ карает за оборот средств платежей, технических устройств и компьютерных программ, если они «предназначены для неправомерного осуществления приема, передачи, выдачи, перевода денежных средств», а электронные средства платежа передаются для «осуществления неправомерных операций» (ч.ч. 3 и 4 ст. 187 УК РФ).

Ранее нами уже приводились аргументы о допустимости признания «способствования совершению абстрактного преступления без осведомленности о его конкретном виде и исполнителе, не являющегося соучастием», перспективной прикосновенностью к последующему посягательству. Такой прием «эшелонирует охрану наиболее значимых общественных отношений, направлен на предупреждение причинения им вреда» [6]. Обслуживание абонентского терминала в целях совершения преступления предполагает фактическое участие субъекта, деяние которого квалифицируется по ст. 274.3 УК РФ, в мошенничествах, диверсиях и иных посягательствах, которые становятся возможными благодаря маскировке и анонимизации их исполнителей [7, 8, 9]. При этом личное знакомство фигурантов, объединяющихся в группы, в том числе организованные, необязательно. Об этом свидетельствует практика рассмотрения судами дел, связанных с незаконным оборотом наркотических средств. Так, согласно разъяснениям кассационного суда, то обстоятельство, «что осуждённые при совершении инкриминированных преступлений осуществляли разработанный неустановленным лицом план, не противоречит выводу суда о совершении преступления ... в группе лиц по предварительному сговору друг с другом»¹. В другом случае была подтверждена верность тезиса об осуществлении осуждённым в составе группы «противозаконной деятельности, связанной со сбытом марихуаны, в ходе которой он по предварительной договорен-

ности с незнакомым лицом после получения от него сообщения о месте нахождения наркотика забрал свертки с марихуаной, одну часть по указанию данного лица поместил по вышеуказанному адресу»².

Заметим, что на практике «цель совершения преступления» толкуется расширительно. Обратим внимание на такую ситуацию: «По версии следствия ... обвиняемый согласился на предложение о заработке от анонимного куратора в мессенджере и вошел в состав группы, занимавшейся телефонными мошенничествами. Мужчина следил за работой абонентских терминалов пропуска голосового трафика (сим-боксов) в съемных квартирах... За время работы злоумышленник использовал более 4,5 тысячи сим-карт»³. В приведенном примере целью виновного в незаконном использовании абонентского терминала было создание условий для совершения серии преступлений, а именно мошенничеств. Он обоснованно не признан соучастником всех мошенничеств, совершенных организованной группой. Для такого понимания диспозиции ч. 1 ст. 274.3 УК РФ есть основания, так как в противном случае дополнение уголовного закона указанной нормой следовало бы признать избыточным. Она восполняет существовавший ранее пробел, когда отсутствовали основания для привлечения к ответственности лиц, которые осознавали, что содействуют преступной деятельности, но не были осведомлены о времени, месте и способах конкретных посягательств, то есть не являлись соучастниками. В целом о ст.ст. 274.3-274.5 УК РФ М.М. Лапунин пишет, как о нормах с двойной превенцией: «...выявляя и пресекая подобные общественно опасные деяния, правоохранительные органы снижают вероятность совершения в дальнейшем более тяжких преступлений» [10, с. 193].

С учетом изложенного требует комментария и такой квалифицированный состав, как незаконное использование абонентского терминала «организованной группой» (ч. 3 ст. 274.3 УК РФ). Вполне обоснованным будет применение данной нормы в отношении каждого из участников организованных групп мошенников, террористов или диверсантов, которые при совершении преступлений осознавали, что используют абонентский терминал или виртуальную телефонную станцию [11, 12]. Что касается субъекта, лишь обеспечивающего функционирование терминала, но не являющегося соучастником совершаемых с его использованием мошенничеств и иных преступлений, то его следует рассматривать именно как участника организованной группы лиц, использующих данный терминал [13]. Например, следствие квалифицировало только по ч. 3 ст. 274.3 УК РФ действия гражданина, который «откликнулся на предложение в интернете и получил от вербовщиков необходимую технику. В квартирах он устано-

¹ Определение Первого кассационного суда общей юрисдикции от 29.04.2025 № 77-1486/2025 (УИД 52RS0007-01-2020-003085-04).

² Кассационное определение Второго кассационного суда общей юрисдикции от 12.12.2024 № 77-3439/2024 (УИД 77RS0031-02-2023-008531-03).

³ Голубев Ф. Прокуратура направила в суд дело о незаконном использовании абонентского терминала // Дзен: сайт. 14.04.2026 // URL: <https://dzen.ru/a/ad3ijZBYQg6Gh-ZQ> (дата обращения: 24.05.2026).

вил четыре сим-боксы не менее чем на 1000 сим-карт различных операторов связи и обеспечивал их бесперебойное функционирование, получая за это еженедельно 500 долларов США». Терминалы использовались «дистанционными мошенниками с целью обмана граждан»¹. В другом случае, «по данным следствия, ... двое несовершеннолетних, действуя по указанию третьих лиц, обеспечивали непрерывную работу устройства SIM-боксы, позволяющего совершать массовые звонки и отправлять сообщения от имени разных абонентов, тем самым поддерживая функционирование мошеннической схемы, направленной на обман граждан и хищение их денежных средств»². Заметим, что в обоих случаях субъекты, обеспечивающие функционирование терминалов, не были признаны соучастниками мошенничества, даже с учетом того, что оно совершалось организованными группами. Соответствует реальности и тот тезис, согласно которому лица, совершающие имущественные преступления с использованием абонентских терминалов, объединяются для посягательств именно на отношения собственности. Поэтому, если есть осознание соответствующего обстоятельства, то функционирование терминала обеспечивается скорее не организованной группой, а в интересах организованной группы. Например, в Уголовном кодексе Кыргызской Республики установлена ответственность за совершенные «в интересах организованной преступной группы» коррупционные деяния (ч. 2 ст. 336 УК КР) и превышение власти (п. 3 ч. 2 ст. 338 УК КР).

Сложно поддержать законодателя, когда он использует в ч. 1 ст. 274.3 УК РФ два таких криминообразующих признака как «цель совершения преступлений» и «тяжкие последствия». Во-первых, именно в создании условий для совершения других преступлений состоят фактические вредные последствия незаконного обеспечения функционирования абонентского терминала. Во-вторых, традиционно уголовно-правовое содержание тяжких последствий предполагает применение данной категории для дифференциации ответственности и используется при конструировании составов с отягчающими и особо отягчающими обстоятельствами [14]. Например, в преступлениях, предусмотренных ст.ст. 272-274.1 УК РФ, которые также как и обеспечение функционирования или использование абонентского терминала, могут состоять в модификации информации, под тяжкими последствиями предлагается «понимать, в частности, длительную приостановку или нарушение работы предприятия, учреждения или организации, получение доступа к информации, составляющей охраняемую законом тайну, предоставление к ней доступа неограниченному кругу

лиц, причинение по неосторожности смерти, тяжкого вреда здоровью хотя бы одному человеку и т.п.»³. Но применительно к ч. 1 ст. 274.3 УК РФ подобное толкование «тяжких последствий» вряд ли возможно.

Общественную опасность рассматриваемого преступления С.В. Кравчук усматривает в первую очередь в посягательстве «на установленный порядок функционирования телекоммуникационной инфраструктуры, являющейся критически значимым элементом информационной безопасности государства и жизнеобеспечения общества» [15, с. 131]. Формирование представления о содержании вреда и, соответственно, «тяжких последствиях» незаконного использования и обеспечения функционирования абонентского терминала предполагает конкретизацию угрозы безопасности, создаваемой данным преступлением. При этом было бы неверно строго отождествлять тяжкие последствия преступления, предусмотренного ч. 1 ст. 274.3 УК РФ, с последствиями посягательств, в целях совершения которых абонентский терминал используется и обслуживается. Хотя, например, в случае совершения разбоя, сопряженного с убийством, действия виновного квалифицируются по двум составам преступлений с отягчающими обстоятельствами (п. «в» ч. 4 ст. 162 УК РФ и п. «з» ч. 2 ст. 105 УК РФ): убийство повышает общественную опасность разбоя, а разбой отягчает убийство. О наличии тяжких последствий могли бы свидетельствовать, например, масштабы незаконного использования абонентского терминала, общее количество совершенных с его использованием посягательств, количество пострадавших, а возможно, и особая мера вреда, причиненного безопасности общества и государства. В отдельных случаях тяжкими последствиями могут быть признаны совершенные с использованием абонентского терминала или виртуальной телефонной станции террористический акт, диверсия, посягательство на жизнь государственного деятеля.

В уголовном праве уже сформирована парадигма, согласно которой использование информационных технологий значительно повышает общественную опасность посягательств. Данный тезис не исключает того, что и степень опасности преступлений, совершаемых с незаконным использованием абонентского терминала пропуска трафика посредством интернета, может послужить основанием для дифференциации ответственности за их совершение.

ЗАКЛЮЧЕНИЕ

Результаты проведенного анализа признаков составов преступлений, предусмотренных ст. 274.3 УК РФ, позволили сформулировать ряд выводов,

¹ В Твери раскрыли терминалы пропуска трафика для мошенничеств «на дому» // РИА «Новости»: сайт. 05.12.2025 // URL: <https://ria.ru/20251205/moshenniki-2060168169.html> (дата обращения: 21.06.2026).

² В Нижегородской области двое несовершеннолетних обвиняются в незаконном использовании абонентского терминала пропуска трафика // Следственное управление Следственного комитета Российской Федерации по Нижегородской области: сайт. 03.03.2026 // URL: <https://nnovgorod.sledcom.ru/news/item/2066816/> (дата обращения: 21.06.2026).

³ См. п. 14 Постановления Пленума Верховного Суда Российской Федерации от 15.12.2022 № 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».

имеющих теоретическое и правоприменительное значение.

Прежде всего, в доктрине и судебной практике обоснованно выделяются три самостоятельных способа совершения посягательств рассматриваемого вида: использование при совершении преступления абонентского терминала пропуска трафика, обслуживаемого иным лицом; собственно обслуживание такого терминала для совершения преступлений другими лицами; использование абонентского терминала для совершения преступления лицом, которое одновременно обеспечивает его функционирование. Указанная дифференциация имеет принципиальное значение для правильной квалификации действий каждого из участников группы и позволяет разграничить их роли в условиях распределенной цифровой инфраструктуры.

Особого внимания заслуживает толкование цели совершения «иного преступления» как обязательного элемента субъективной стороны анализируемой нормы. Считаем, что данная цель характерна не только для лиц, непосредственно использующих терминал для совершения конкретных посягательств, но и для тех, кто обеспечивает его бесперебойное функционирование. В отношении последней категории субъектов цель должна толковаться расширительно: достаточно осознания виновным того, что осуществляемая им деятельность по обслуживанию терминала объективно создает условия для совершения неопределенным кругом лиц общественно опасных деяний в сфере информационно-телекоммуникационных технологий. Противоположный подход – узкое, буквальное толкование цели применительно к лицам, лишь обеспечивающим функционирование терминала, – нивелировал бы основной смысл ст. 274.3 УК РФ, а именно криминализацию деятельности по созданию условий для совершения

иных преступлений, в тех случаях, когда признаки соучастия (совместность, сговор, конкретизация преступного намерения) отсутствуют либо не могут быть доказаны в силу анонимности и территориальной распределенности субъектов.

Наконец, также требуют системного подхода критерии наступления «тяжких последствий» как альтернативного основания ответственности. Представляется, что о наличии таких последствий могут свидетельствовать масштаб противоправной деятельности, опосредованной использованием терминала (объем пропущенного трафика, длительность функционирования); множественность совершённых с его использованием посягательств и значительное число пострадавших; а также характер причиненного вреда, в частности, если такой вред затрагивает основы безопасности личности, общества и государства. В особо опасных случаях тяжкими последствиями надлежит признавать совершённые с использованием терминала или виртуальной телефонной станции террористический акт, диверсию, посягательство на жизнь государственного деятеля, поскольку данные деяния создают угрозу охраняемым конституционным ценностям и влекут необратимые социально-политические последствия.

Таким образом, изложенные выводы позволяют уточнить уголовно-правовую квалификацию деяний, предусмотренных ст. 274.3 УК РФ, и могут быть использованы в целях совершенствования правоприменительной практики, а также для дальнейшей теоретической разработки проблем противодействия цифровой преступности. Перспективными направлениями исследований видятся выработка единых критериев оценки тяжести последствий и определение пределов расширительного толкования цели «совершения иного преступления» применительно к различным категориям субъектов. ■

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Алексеева А.П., Ничуговская О.Н. Киберпреступность: основные черты и формы проявления // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. 2017. № 1. С. 27-34.
2. Случевская Ю.А. Цифровые технологии в предупреждении экологической преступности: оценка эффективности и рисков применения // Викиматология. 2025. Т. 12. № 4. С. 576-588.
3. Поляков А.В., Гринева Д.А. О возможностях использования информационных технологий в решении задач оперативно-розыскной деятельности // Межведомственный научно-практический Петербургский оперативно-розыскной форум: Материалы межведомственной научно-практической конференции. СПб: СПбУ МВД России, 2025. С. 211-215.
4. Алексеева А.П., Анисимова Т.В. Законодательные инициативы в сфере установления уголовной ответственности за незаконные использование и передачу, сбор и хранение компьютерной информации, содержащей персональные данные: проблемы и перспективы // Уголовное законодательство: вчера, сегодня, завтра: Материалы международной научно-практической конференции. СПб: СПбУ МВД России, 2024. С. 13-15.
5. Кравчук С.В. Техничко-правовая характеристика абонентского терминала пропуска трафика и виртуальной телефонной станции как предметов преступления // International Law Journal. 2025. Т. 8. № 8. С. 252-262.
6. Борков В.Н. Перспективная прикосновенность к преступлению // Вестник Сибирского юридического института МВД России. 2025. № 4. С. 9-15.
7. Глубоковских Р.В., Гринева Д.А. Характеристика оперативно-розыскного инструментария при раскрытии хищения денежных средств с банковских счетов // XIII Балтийский юридический форум «Закон и правопорядок в третьем тысячелетии»: Материалы международной научно-практической конференции. Калининград: КФ СПбУ МВД России, 2025. С. 25-27.

8. Попов С.В. К вопросу об особенностях обнаружения признаков мошеннических действий в сети Интернет // Межведомственный научно-практический Петербургский оперативно-розыскной форум: Материалы межведомственной научно-практической конференции. СПб: СПбУ МВД России, 2025. С. 216-219.

9. Поляков А.В., Гринева Д.А. О возможностях использования информационных технологий в решении задач оперативно-розыскной деятельности // Межведомственный научно-практический Петербургский оперативно-розыскной форум: Материалы межведомственной научно-практической конференции. СПб: СПбУ МВД России, 2025. С. 211-215.

10. Лапунин М.М. Уголовно-правовые запреты относительно оборота средств, используемых для посягательств в сфере компьютерной информации: законодательные новеллы и их потенциал // Вестник Саратовской государственной юридической академии. 2025. № 5. С. 191-198.

11. Погорелова К.Р., Пахомова О.Н. Призывы к экстремистской деятельности: проблемы квалификации и назначения уголовного наказания // Современность в творчестве начинающего исследователя: Материалы научно-практической конференции. Иркутск: ВСИ МВД России, 2024. С. 175-178.

12. Попов С.В. К вопросу о нормативно-правовом регулировании в сфере противодействия экстремизму // X Балтийский юридический форум «Закон и правопорядок в третьем тысячелетии»: Материалы международной научно-практической конференции. Калининград: КФ СПбУ МВД России, 2022. С. 63-64.

13. Пахомова О.Н. Актуальные проблемы квалификации преступлений в кредитной сфере // IX Балтийский юридический форум «Закон и правопорядок в третьем тысячелетии»: Материалы международной научно-практической конференции. Калининград: КФ СПбУ МВД России, 2021. С. 67-68.

14. Случевская Ю.А. Компенсационная и восстановительная функции уголовного права // Вестник Санкт-Петербургского университета МВД России. 2024. № 4 (104). С. 194-208.

15. Кравчук С.В. К вопросу о социальной обусловленности криминализации незаконного использования абонентского терминала пропуска трафика или виртуальной телефонной станции // Проблемы права. 2025. № 4. С. 129-138.

REFERENCES

1. Alekseyeva A.P., Nichugovskaya O.N. Kiberprestupnost': osnovnyye cherty i formy proyavleniya // Prestupnost' v sfere informatsionnykh i telekommunikatsionnykh tekhnologiy: problemy preduprezhdeniya, raskrytiya i rassledovaniya prestupleniy. 2017. № 1. S. 27-34.

2. Sluchevskaya Yu.A. Tsifrovyye tekhnologii v preduprezhdenii ekologicheskoy prestupnosti: otsenka effektivnosti i riskov primeneniya // Viktimologiya. 2025. T. 12. № 4. S. 576-588.

3. Polyakov A.V., Grineva D.A. O vozmozhnostyakh ispol'zovaniya informatsionnykh tekhnologiy v reshenii zadach operativno-rozysknoy deyatel'nosti // Mezhvedomstvennyy nauchno-prakticheskiy Peterburgskiy operativno-rozysknoy forum: Materialy mezhvedomstvennoy nauchno-prakticheskoy konferentsii. SPb: SPbU MVD Rossii, 2025. S. 211-215.

4. Alekseyeva A.P., Anisimova T.V. Zakonodatel'nyye initsiativy v sfere ustanovleniya ugolovnoy otvetstvennosti za nezakonnyye ispol'zovaniye i peredachu, sbor i khraneniye komp'yuternoy informatsii, sodержashchey personal'nyye dannyye: problemy i perspektivy // Ugolovnoye zakonodatel'stvo: vchera, segodnya, zavtra: Materialy mezhdunarodnoy nauchno-prakticheskoy konferentsii. SPb: SPbU MVD Rossii, 2024. S. 13-15.

5. Kravchuk S.V. Tekhniko-pravovaya kharakteristika abonentskogo terminala propuska trafika i virtual'noy telefonnoy stantsii kak predmetov prestupleniya // International Law Journal. 2025. T. 8. № 8. S. 252-262.

6. Borkov V.N. Perspektivnaya prikosnovennost' k prestupleniyu // Vestnik Sibirskogo yuridicheskogo instituta MVD Rossii. 2025. № 4. S. 9-15.

7. Glubokovskikh R.V., Grineva D.A. Kharakteristika operativno-rozysknogo instrumentariya pri raskrytii khishcheniya denezhnykh sredstv s bankovskikh schetov // XIII Baltiyskiy yuridicheskiy forum «Zakon i pravoporyadok v tret'eyem tysyacheletii»: Materialy mezhdunarodnoy nauchno-prakticheskoy konferentsii. Kaliningrad: KF SPbU MVD Rossii, 2025. S. 25-27.

8. Popov S.V. K voprosu ob osobennostyakh obnaruzheniya priznakov moshennicheskikh deystviy v seti Internet // Mezhvedomstvennyy nauchno-prakticheskiy Peterburgskiy operativno-rozysknoy forum: Materialy mezhvedomstvennoy nauchno-prakticheskoy konferentsii. SPb: SPbU MVD Rossii, 2025. S. 216-219.

9. Polyakov A.V., Grineva D.A. O vozmozhnostyakh ispol'zovaniya informatsionnykh tekhnologiy v reshenii zadach operativno-rozysknoy deyatel'nosti // Mezhvedomstvennyy nauchno-prakticheskiy Peterburgskiy operativno-rozysknoy forum: Materialy mezhvedomstvennoy nauchno-prakticheskoy konferentsii. SPb: SPbU MVD Rossii, 2025. S. 211-215.

10. Lapunin M.M. Ugolovno-pravovyye zaprety otnositel'no oborota sredstv, ispol'zuyemykh dlya posyagatel'stv v sfere komp'yuternoy informatsii: zakonodatel'nyye novelly i ikh potentsial // Vestnik Saratovskoy gosudarstvennoy yuridicheskoy akademii. 2025. № 5. S. 191-198.

11. Pogorelova K.R., Pakhomova O.N. Prizvyv k ekstremistskoy deyatel'nosti: problemy kvalifikatsii i naznacheniya ugolovnogo nakazaniya // Sovremennost' v tvorchestve nachinayushchego issledovatelya: Materialy nauchno-prakticheskoy konferentsii. Irkutsk: VSI MVD Rossii, 2024. S. 175-178.

12. Popov S.V. K voprosu o normativno-pravovom regulirovanii v sfere protivodeystviya ekstremizmu // X Baltiyskiy yuridicheskiy forum «Zakon i pravoporyadok v tret'yem tysyacheletii»: Materialy mezhdunarodnoy nauchno-prakticheskoy konferentsii. Kaliningrad: KF SPbU MVD Rossii, 2022. S. 63-64.

13. Pakhomova O.N. Aktual'nyye problemy kvalifikatsii prestupleniy v kreditnoy sfere // IX Baltiyskiy yuridicheskiy forum «Zakon i pravoporyadok v tret'yem tysyacheletii»: Materialy mezhdunarodnoy nauchno-prakticheskoy konferentsii. Kaliningrad: KF SPbU MVD Rossii, 2021. S. 67-68.

14. Sluchevskaya Yu.A. Kompensatsionnaya i vosstanovitel'naya funktsii ugovnogo prava // Vestnik Sankt-Peterburgskogo universiteta MVD Rossii. 2024. № 4 (104). S. 194-208.

15. Kravchuk S.V. K voprosu o sotsial'noy obuslovlennosti kriminalizatsii nezakonnogo ispol'zovaniya abonentskogo terminala propuska trafika ili virtual'noy telefonnoy stantsii // Problemy prava. 2025. № 4. S. 129-138.

© Борков В.Н., 2026.

ССЫЛКА ДЛЯ ЦИТИРОВАНИЯ

Борков В.Н. Особенности и правила квалификации незаконного использования абонентского терминала пропуска трафика // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. 2026. № 3 (85). С. 9-16.