Дата поступления рукописи в редакцию: 04.10.2026 г. DOI: 10.24412/2224-9133-2026-10-677-682
Дата принятия рукописи в печать: 10.11.2026 г.

СТРАНЦОВ Алексей Алексеевич,
старший преподаватель кафедры гражданско-правовых дисциплин БЮИ МВД России, подполковник полиции,
e-mail: strancovaa@buimvd.ru

ОБЩЕСТВЕННАЯ ОПАСНОСТЬ ОРГАНИЗАЦИИ НЕЗАКОННОЙ ДЕЯТЕЛЬНОСТИ ПО ПЕРЕДАЧЕ АБОНЕНТСКИХ НОМЕРОВ ПОДВИЖНОЙ РАДИОТЕЛЕФОННОЙ СВЯЗИ

Аннотация. *Статья посвящена рассмотрению характера и степени общественной опасности деяния, предусмотренного статьей 274.4 УК РФ, введенной в действие с 1 сентября 2025 года. Анализируется обоснование криминализации организации незаконной деятельности по передаче абонентских номеров подвижной радиотелефонной связи, учитывая необходимость противодействия росту дистанционных преступлений и борьбой с телефонным мошенничеством. Предлагается использование нового понятия «сим-дроппинг» для обозначения организации незаконной деятельности по передаче абонентских номеров подвижной радиотелефонной связи. Изучается вопрос о категории рассматриваемого преступления, связанного с его массовым использованием в криминальных схемах, вовлечением граждан в противоправную деятельность, подрывом информационной безопасности и доверия к связи в России.*

Ключевые слова: *корыстная заинтересованность, общественная опасность, подвижная радиотелефонная связь, передача абонентских номеров, сим-карты, преступления в сфере компьютерной информации, уголовная ответственность.*

Для цитирования: *Странцов А. А. Общественная опасность организации незаконной деятельности по передаче абонентских номеров подвижной радиотелефонной связи // Право и управление. 2026. № 10. С. 677–682.*

STRANTSOV Alexey Alekseevich,
Senior Lecturer of the Department of Civil Law Disciplines of the Law Institute of the Ministry of Internal Affairs of Russia, Police Lieutenant Colonel

PUBLIC DANGER OF ORGANIZING THE ILLEGAL TRANSFER OF MOBILE SUBSCRIBER NUMBERS

Annotation. *The article examines the nature and degree of public danger of the offense provided for by Article 274.4 of the Criminal Code of the Russian Federation, which came into force on September 1, 2025. It analyzes the rationale behind criminalizing the organization of illegal activities involving the transfer of mobile radiotelephone subscriber numbers, taking into account the need to counter the rise in remote crimes and combat phone fraud. It is proposed to use the new term «SIM-dropping» to denote the organization of illegal activities involving the transfer of mobile radiotelephone communication numbers. The study explores the categorization of the crime in question, linking it to its mass utilization in criminal schemes, the involvement of citizens in illegal activities, and the undermining of information security and public trust in telecommunications in Russia.*

Key words: *self interested motivation, public danger, mobile radiotelephone communication, transfer of subscriber numbers, SIM cards, cybercrimes, criminal liability.*

For citation: *Strantsov A. A. Public danger of organizing the illegal transfer of mobile subscriber numbers. Law and administration. 2026;(10):677–682. (In Russ.).*

В современный период существования социума информационные технологии и связь по сравнению с другими общественными сферами развиваются экспоненциально быстро, так как новые технологии не просто сменяют старые, а ускоряют появление следующих. Долгое время развитие процессоров подчинялось Закону Мура [1], по которому удвоение количества транзисторов на чипе происходило каждые два года. На сегодня классический кремний уже подходит к своим физическим границам, но скорость вычислений продолжает расти за счет новых архитектур, в частности суперкомпьютеров и искусственного интеллекта. Актуальным трендом является конвергенция (слияние) технологий, когда облачные вычисления, сверхбыстрая связь (5G) и искусственный интеллект объединяются, что приводит не к постепенным, а лавинообразным изменениям в различных областях общественной жизни.

Отмеченные выше скоростные преобразования технологий в области связи, в свою очередь, создают благоприятные условия для появления новых общественно опасных деяний, которым сложно противостоять по причине их искусственной анонимности и трансграничного характера совершения таковых. На территории государства возникает повсеместная ситуация, при которой злоумышленники, в том числе активизируясь за рубежом, адаптируются к использованию технологий быстрее, чем законодательные органы власти и правоохранительная система в целом. К таким противоправным деяниям, обладающим значительной вредоносностью, следует отнести преступления в сфере компьютерной информации (киберпреступления). При этом отмечается высокий удельный вес преступлений, совершаемых с использованием информационно-телекоммуникационных технологий (около 40%), и ежегодный неуклонный рост этого показателя (10-15%) [2].

Дополнительный фактор, повышающий общественную опасность подобных правонарушений помимо высокоразвитых современных технологий, заключается в возможности применения методов социальной инженерии в совокупности с территориальной отдаленностью. Телефонные мошенники и создатели фишинговых сайтов используют приемы психологического воздействия – страх, спешку, авторитет правоохранительных органов (полиции, Росгвардии, ФСБ, ФССП и др.) и (или) известных кредитных организаций (Сбербанк, Т-банк и т.д.). Преступный успех также может быть вызван цифровой и правовой неграмотностью потерпевших, тяжелым финансовым положением, а также их сложной жизненной ситуацией. При этом злоумышленник может находиться в другом населенном пункте, регионе, иностранном государстве, создавая себе анонимность, ощущая себя заведомо безнаказанно и уверенно нарушая права, законные интересы физических, юридических лиц, публично-правовых образований на территории России. Организованные преступные группы создают разветвленные схемы незаконного оборота абонентских номеров, используемых в качестве инструмента для совершения хищений, вымогательств, незаконного сбора персональных данных и иных противоправных деяний [3, с. 74].

Особо негативная ситуация возникает при функционировании организованной преступной группы за рубежом, что закономерно осложняет получение информации для расследования уголовного дела, когда официальные международные запросы согласовываются и направляются в течение более длительного времени, чем период удаления возможных доказательств о причастности к совершению определенного киберпреступления. Учитывая проведение Россией Специальной Военной Операции (СВО), должностные лица в некоторых государствах (Украина, Польша, Швеция, Канада и др.) умышленно игнорируют факты совершения преступных деяний, если таковые направлены против российских граждан.

С учетом названных аспектов возрастающей общественной опасности киберпреступлений и с целью эффективного противодействия совершению как криминальных деяний в сфере компьютерной информации, так и иных преступных посягательств (мошенничество, вымогательство, экстремизм, диверсии и т. д.) Федеральным законом от 31.07.2025 № 282-ФЗ с 1 сентября 2025 года введена в действие ст. 274.4 УК РФ, устанавливающая уголовную ответственность за организацию незаконной деятельности по передаче абонентских номеров подвижной радиотелефонной связи, а также участия в такой деятельности при наличии корыстной заинтересованности или с целью совершения иного преступления. Социальная и правовая ценность новой уголовно-правовой нормы, на взгляд автора, не вызывает сомнений, поскольку организация противоправной деятельности по торговле абонентскими номерами подвижной радиотелефонной связи без реальной идентификации или регистрации на фактического пользователя в обход официального контроля (так называемые «серые» сим-карты), прямо или косвенно направлена на создание криминальной инфраструктуры для последующего совершения тяжких и особо тяжких преступлений. Такие сим-карты оформляются на паспортные данные дропперов или через корпоративные контракты фиктивных фирм-однодневок, чтобы в дальнейшем осуществить попытку скрыть личность лица, использующего сотовую связь для противоправных целей при совершении телефонных звонков или использовании ресурсов сети

«Интернет». Посредники, иногда не подозревая, что нарушают законодательный запрет, распространяют сим-карты в торговых центрах, на улицах, онлайн, через курьеров без заключения предусмотренного законодательством официального договора с абонентом подвижной радиотелефонной связи.

Дроппер (дроп) – это сложившееся в финансовой и юридической практике общеизвестное понятие, определяющее субъекта умышленного либо неосторожного криминального посредничества, который предоставляет свои банковские карты, реквизиты или доступ к онлайн-банку для поддержания оборота (перечисления) денежных средств, полученных незаконным путем. Исходя из факта заимствования названного термина из английского языка, автор полагает, что более корректно понятие «дроппер» как субъект действия (существительное «dropper»), чем «дроп» как само действие (глагол «drop»). Дропперство может быть как осознанным, так и случайным (невольным). В первом случае дропперы понимают, что участвуют в преступной схеме, и выполняют свою роль ради корыстной заинтересованности, что может быть выражено, в том числе в возмездной передаче сим-карт, зарегистрированных с использованием их персональных данных. Во второй ситуации дропперами становятся потерпевшие, введенные в заблуждение, то есть в отношении которых был реализован противоправный замысел. Речь идет, как правило, о людях, поверивших в «легкий заработок» («менеджер по переводам», «финансовый консультант» и т. д.), либо те, кому якобы ошибочно перевели деньги на банковскую карту с просьбой вернуть владельцам, но уже на другой банковский счет.

Учитывая факты выявления в российской правовой реальности деятельности дропперов, умышленно предоставляющих свои абонентские номера для совершения противоправных действий, то с целью обозначения незаконной деятельности по распространению «серых» сим-карт, предлагается ввести в сферу юридической кибербезопасности термин «сим-дроппинг», который, в отличие от «сим-свопинга» (подмена сим-карты), в настоящее время еще не применялся. Термины «сим-делегация» или «сим-пушинг» имеют схожее с «сим-дроппингом» значение, но не подходят для наименования противоправной деятельности, так как могут являться вполне законными операциями с сим-картами. Не вполне отражает конкретную сущность рассматриваемого уголовно наказуемого явления и термин «сим-фрод», по причине его более абстрактного определения общей сферы телефонных мошенничеств. Предлагаемое понятие «сим-дроппинг» подразумевает не только устоявшийся негативный смысл в понимании граждан России (криминальные схемы с участием подставных лиц), но и организованность, системность, массовость незаконного распространения сим-карт, как правило, для совершения иных противоправных действий.

Характер и степень общественной опасности сим-дроппинга заключается в создании теневого рынка сим-карт, существование которого подрывает информационную безопасность и доверие к связи, когда при звонке с незнакомого номера принимающий абонент привычно игнорирует вызов, по умолчанию предполагая, что может быть таргетирован атакой мошенников. Нелегальный оборот номеров нарушает установленный государством порядок идентификации абонентов и в целом дестабилизирует работу телекоммуникационной сферы общества, снижая ее ценность, так как передача сим-карт неустановленным лицам деструктивирует систему обязательной идентификации абонентов. При такой ситуации государство и мобильные операторы теряют возможность реализовывать функции контроля в отношении подвижной радиотелефонной связи, чем активно пользуются участники преступных групп и сообществ, которые как правило, лично не знакомы, не осведомлены о конкретных посягательствах, применяемых орудиях и средствах [4, с. 15].

Незаконная передача сим-карт с абонентскими номерами, оформленными на других лиц, обеспечивает анонимизацию злоумышленников, позволяет преступникам скрывать свою реальную личность при телефонных звонках потенциальным жертвам, что существенно затрудняет оперативно-розыскные мероприятия и успешное расследование киберпреступлений. Организаторы рассматриваемой незаконной деятельности, как правило, используют обман, обещания заработка, провоцируя людей оформлять на себя десятки номеров для их дальнейшей передачи в руки преступников.

При этом начальной целевой аудиторией для осуществления сим-дроппинга, как правило, являются представители молодежи и уязвимых групп населения, которые вербуются посредством соцсетей или мессенджеров под предложением якобы легальной подработки, фактически склоняя граждан к совершению преступлений. Так, в производстве ОРП УМВД СУ УМВД России по г. Липецку находится уголовное дело № 126014200.24000117 по подозрению несовершеннолетних ФИО7 и ФИО8, ФИО1 и неустановленных лиц в совершении преступлений, предусмотренных ч. 2 ст. 274.4, ч. 1 ст. 159, ч. 3 ст. 30, ч. 3 ст. 159, ч. 4 ст. 159 УК РФ. Вместе с тем, на момент рассмотрения судом апелляционной инстанции апелляционной жалобы на постановление об избрании меры пресечения изменились основания, учитываемые судом при решении вопроса об

избрании меры пресечения, а именно согласно постановлению о предъявлении обвинения ФИО1 6 августа 2026 г. ей предъявлено обвинение в совершении преступления, предусмотренного ч. 2 ст. 274.4 УК РФ, относящегося к категории небольшой тяжести [5].

Анализируя санкции, содержащиеся в ч. 1 и ч. 2 ст. 274.4 УК РФ можно сделать вывод, что и организацию сим-дроппинга, и участие в нем законодатель отнес к преступлениям небольшой тяжести (до 3-х, до 2-х лет лишения свободы соответственно). Обращаясь к судебной практике, которая еще только складывается, отметим наметившуюся тенденцию вынесения обвинительных приговоров по ст. 274.4 УК РФ, то есть уголовно-правовая норма уверенно применяется в отношении участников сим-дроппинга. Так, например, Демским районным судом г. Уфы Республики Башкортостан по делу № 1-126/2026 установлено, что участники организованной группы заведомо объединились для совершения преступлений, действовали сплоченно, соблюдали конспирацию с целью сокрытия преступной деятельности, выраженную во взаимодействии и обмене информацией исключительно через интернет-мессенджер «данные изъяты», организованная группа осуществляла преступную деятельность под единым руководством, имела строгую иерархию участников с распределением между ними определенных ролей, направленных на выполнение каждым участником определенных функций, участники организованной группы взаимодействовали с целью реализации единого преступного умысла и получали имущественную выгоду от совершенных преступлений.

Структура организованной группы предполагала включение в свой состав дропповодов, отвечающих за подбор дроппов, на кого оформляются банковские счета, а также абонентские номера, используемые для перечисления денежных средств, добытых преступным путем, обналичивание указанных денежные средства (дроп-повод, курьер, забирающий банковские карты, обнальщик). Не позднее ДД.ММ.ГГГГ, находясь по адресу: «адрес», следуя указаниям неустановленных в ходе следствия лиц, используя вышеперечисленное подключенное ранее оборудование, Д.Д.А. поместил полученные ранее от неустановленных в ходе следствия лиц 32 сим-карты оператора сотовой связи ПАО «МТС» с абонентскими номерами, зарегистрированные на третьих лиц, не осведомленных о преступных намерениях преступной группы, о чем уведомил неустановленных соучастников для совершения хищения денежных средств граждан России [6]. Суд квалифицировал действия Д.Д.А. по факту участия в деятельности по передаче абонентских номеров с нарушением требований законодательства Российской Федерации – по ч. 2 ст. 274.4 УК РФ, и назначил наказание в виде 8 месяцев принудительных работ с удержанием 5% заработной платы в доход государства.

В научной литературе указывается, что если лицо передает не чужие, а свои абонентские номера, он выступает субъектом не преступления, предусмотренного ст. 274.4 УК РФ, а административного правонарушения, предусмотренного ст. 13.29.1 КоАП РФ [7]. Исходя из оснований криминализации сим-дроппинга, автор не вполне согласен с указанной позицией. Рассмотрим следующий пример уголовного дела. Димитровский районный суд г. Костромы Костромской области по делу № 1-99/2026 установил, что Л.А.А, находясь в достоверно неопределенном месте на территории г. Кострома, из корыстной заинтересованности, в ответ на ранее озвученное Лицами № 1 и № 2 предложение, сообщила последним о готовности личного участия в деятельности по передаче абонентских номеров иным лицам путем оформления на свое имя абонентских номеров, функционирующих посредством технологии виртуальной сим-карты (eSIM), идентифицирующей абонента в сети подвижной радиотелефонной связи оператора «данные изъяты», за денежное вознаграждение, при этом Л.А.А. осознавала, что оформление договоров об оказании услуг подвижной связи с последующей передачей абонентских номеров иным лицам противоречит требованиям законодательства Российской Федерации и установленным Условиям оказания услуг подвижной связи «данные изъяты», а также может способствовать злоумышленникам использовать чужие номера для сокрытия своей личности, совершения преступлений и обхода правовых ограничений. 24.12.2025 Л.А.А. достоверно зная о том, что оформленные на ее имя абонентские номера фактически не будут использоваться ей в дальнейшем, при помощи своего паспорта заключила 16 договоров об оказании услуг подвижной радиотелефонной связи о выделении и предоставлении в пользование абонентских номеров.

В дальнейшем 12.01.2026 подсудимая заключила 14 договоров об оказании услуг подвижной радиотелефонной связи о выделении и предоставлении в пользование абонентских номеров [8]. Суд признал Л.А.А. виновной в совершении преступления, предусмотренного ч. 2 ст. 274.4 УК РФ и назначил ей наказание в виде штрафа в размере 100 000 рублей при ее незаконном заработке за нелегальную передачу сим-карт в размере 10 290 рублей.

Относительно организации незаконной деятельности по передаче сим-карт в судебной практике есть примеры, в которых, на взгляд автора, недооценивается характер и степень общественной опасности сим-дропинга, ввиду то-

го, что рассматриваемое преступление отнесено к категории небольшой тяжести. Так, Дорогомиловским районным судом г. Москвы по делу № 01-0077/2026 в отношении М.Д.Р, обвиняемого в совершении преступления, предусмотренного ч. 1 ст. 274.4 УК РФ, уголовное дело прекращено с учетом тяжести преступления, а также характера совершенного им общественно опасного деяния с назначением меры уголовно - правового характера в виде судебного штрафа [9], который не может превышать половину максимального размера штрафа, предусмотренного санкцией ч. 1 ст. 274.4 КУ РФ.

Таким образом, при сопоставлении характера и степени общественной опасности сим-дроппинга с установленной категорией рассматриваемого преступления, а также учитывая поставленную государством цель по пресечению нелегального оборота сим-карт и ликвидации условий для совершения иных преступных деяний, анонимно и дистанционно направленных против жизни, здоровья, собственности российских граждан, безопасности Российской Федерации, иных публично-правовых образований, в том числе в период проведения СВО, представляется сделать закономерный вывод о том, что отнесение сим-дроппинга к категории преступлений небольшой тяжести является первым шагом в уголовно-правовой политике, но явно недостаточным. Требуется усиление карательной функции уголовной ответственности посредством пересмотра категории рассматриваемого преступления, что напрямую повлияет на увеличение размера санкций, пока еще незначительных, с точки зрения осознания реальной общественной опасности сим-дроппинга в России.

Список литературы:

[1] Мур Г. Э. Прогресс в цифровой интегральной электронике // Материалы Международного совещания IEEE по электронным устройствам. 1975. вып. 21. С. 11–13.

[2] Звечаровский И.Э. Уголовно-правовая политика России на современном этапе // Lex Russica. 2026. № 3. С. 9-16. [Электронный ресурс] // 2026. Доступ из справочной правовой системы «Гарант».

[3] Бегишев И.Р. Уголовно-правовые проблемы криминализации организации деятельности по незаконой передаче абонентских номеров // Законодательство. 2026. № 8. С. 74-80.

[4] Борков В.Н. Перспективная прикосновенность к преступлению // Вестник Сибирского юридического института МВД России. 2025. № 4. С. 9-15.

[5] Апелляционное постановление Липецкого областного суда от 19 августа 2026 г. [Электронный ресурс] // 2026. Доступ из справочной правовой системы «Гарант».

[6] Приговор Демского районного суда г. Уфы Республики Башкортостан от 16 июля 2026 г. по делу № 1-126/2026 [Электронный ресурс] // 2026. Доступ из справочной правовой системы «Гарант».

[7] Сидорова Е.З. Уголовно-правовая характеристика некоторых компьютерных преступлений (статьи 274.3, 274.4 и 274.5 УК РФ) // Вестник Сибирского юридического института МВД России. 2026. № 2. С. 38-44. [Электронный ресурс] // 2026. Доступ из справочной правовой системы «Гарант».

[8] Приговор Димитровского районного суда г. Костромы Костромской области от 28 июля 2026 г. по делу № 1-99/2026 [Электронный ресурс] // 2026. Доступ из справочной правовой системы «Гарант».

[9] Постановление Дорогомиловского районного суда г. Москвы от 05 февраля 2026 г. по делу № 01-0077/2026 [Электронный ресурс] // 2026. Доступ из справочной правовой системы «Гарант».

References:

[1] Moore G.E. Progress in Digital Integrated Electronics // Proceedings of the IEEE International Meeting on Electronic Devices. 1975. issue 21. S. 11-13.

[2] Zvecharovsky I.E. Criminal law policy of Russia at the present stage // Lex Russica. 2026. № 3. S. 9-16. [Electronic resource] // 2026. Access from the Guarantor Reference Legal System.

[3] Begishev I.R. Criminal law problems of criminalizing the organization of illegal transfer of subscriber numbers // Legislation. 2026. № 8. S. 74-80.

[4] Borkov V.N. Perspective touch to the crime // Bulletin of the Siberian Law Institute of the Ministry of Internal Affairs of Russia. 2025. № 4. S. 9-15.

[5] Appeal decision of the Lipetsk Regional Court of August 19, 2026 [Electronic Resource] // 2026. Access from the Guarantor Reference Legal System.

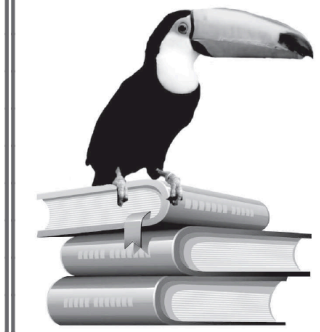
[6] Verdict of the Demsky District Court of Ufa of the Republic of Bashkortostan dated July 16, 2026 in case No. 1-126/2026 [Electronic Resource] // 2026. Access from the Guarantor Reference Legal System.

[7] Sidorova E.Z. Criminal law characteristics of some computer crimes (Articles 274.3, 274.4 and 274.5 of the Criminal Code of the Russian Federation) // Bulletin of the Siberian Law Institute of the Ministry of Internal Affairs of Russia. 2026. № 2. S. 38-44. [Electronic resource] // 2026. Access from the Guarantor Reference Legal System.

[8] The verdict of the Dimitrovsky District Court of Kostroma, Kostroma Region, dated July 28, 2026 in case No. 1-99/2026 [Electronic Resource] // 2026.

Access from the Guarantor Reference Legal System.

[9] Decision of the Dorogomilovsky District Court of Moscow dated February 05, 2026 in case No. 01-0077/2026 [Electronic Resource] // 2026. Access from the Guarantor Reference Legal System.



Юридическое издательство
«ЮРКОМПАНИ»

Издание учебников, учебных и методических пособий, монографий, научных статей.

Профессионально.

В максимально короткие сроки.

Размещаем в РИНЦ, E-Library.

www.law-books.ru