

Дата поступления рукописи в редакцию: 28.09.2026 г.
Дата принятия рукописи в печать: 02.10.2026 г.

DOI: 10.24412/3034-2422-2026-4-140-144

БЕРБЕРОВА Алие Дяверовна,
студентка 3 курса заочной формы обучения,
Российский государственный университет
правосудия имени В.М. Лебедева,
e-mail: mail@law-books.ru

СОВРЕМЕННЫЕ ТЕНДЕНЦИИ РАЗВИТИЯ ЗАКОНОДАТЕЛЬСТВА ОБ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ: ПРИНЯТИЕ ЗАКОНОВ О ВНЕСЕНИИ ИЗМЕНЕНИЙ В УГОЛОВНЫЙ КОДЕКС РОССИЙСКОЙ ФЕДЕРАЦИИ В 2025 И 2026 ГГ.

АННОТАЦИЯ. В статье исследуются изменения и расширения Главы 28 Уголовного кодекса Российской Федерации за период времени с 2025 по 2026 гг. Проводится сравнительный анализ динамики роста преступлений, совершенных с использованием информационно-телекоммуникационных технологий. Анализируется влияние принятых законов о внесении изменений в Уголовный кодекс Российской Федерации на устранение ранее имеющихся проблем правоприменения. Проведена оценка статьи 274.6 Уголовного кодекса Российской Федерации, и её соответствия системе преступлений в сфере компьютерной информации и динамике киберпреступности, определены условия её результативности. Предложены правовые меры для органов расследования, судов и операторов сотовой связи.

КЛЮЧЕВЫЕ СЛОВА: преступления в сфере компьютерной информации, информационно-телекоммуникационные технологии, статья 274.6 УК РФ, административная преюдиция, абонентский номер, идентификатор пользовательского оборудования, подследственность, кибермошенничество.

BERBEROVA Alie Dlavervovna,
3st year student of distance learning,
Russian State University of Justice named after V.M. Lebedev

MODERN TRENDS IN THE DEVELOPMENT OF LEGISLATION ON CRIMINAL LIABILITY FOR CRIMES IN THE FIELD OF COMPUTER INFORMATION: THE ADOPTION OF LAWS AMENDING THE CRIMINAL CODE OF THE RUSSIAN FEDERATION IN 2025 AND 2026

ANNOTATION. The article examines the changes and expansions to Chapter 28 of the Criminal Code of the Russian Federation over the period from 2025 to 2026. A comparative analysis is conducted of the growth dynamics of crimes committed using information and telecommunications technologies. The impact of the adopted laws amending the Criminal Code of the Russian Federation on eliminating previously existing problems in law enforcement is analysed. Article 274.6 of the Criminal Code of the Russian Federation is assessed for its compliance with the system of crimes in the field of computer information and the dynamics of cybercrime, and the conditions for its effectiveness are identified. Legal measures have been proposed for investigative bodies, courts, and mobile network operators.

KEY WORDS: crimes in the field of computer information, information and telecommunications technologies, Article 274.6 of the Criminal Code of the Russian Federation, administrative pre judgment, subscriber number, user equipment identifier, jurisdiction, cyber fraud.

Цифровые технологии сегодня проникли почти во все сферы жизни общества и работы государства. Информация стала одним из ключевых ресурсов, а ее защита — важной составляющей национальной безопасности. В Рос-

сии правовые нормы, которые регулируют обмен информацией, пока только формируются. Переломным моментом стало то, что информационную безопасность включили в число обязательных составляющих национальной безопасности

Российской Федерации [6, с. 57]. Поэтому вопрос уголовной ответственности за преступления в сфере компьютерной информации сейчас особенно актуален. Технологии развиваются стремительно, и законодательство должно успевать за этим ростом: нужны ясные составы преступлений, понятные правила квалификации и предсказуемые решения для правоохранительных органов, следствия и суда.

В 2025–2026 годах законодатель целенаправленно внес изменения в Главу 28 Уголовный кодекс Российской Федерации (далее по тексту – УК РФ): появились новые составы, а действующие нормы стали шире и точнее. Это связано и с усилением охраны персональных данных и информационной инфраструктуры, и с тем, что в уголовном праве необходимо учитывать информационно-телекоммуникационных технологий (далее по тексту – ИТТ) и генеративные модели [2, с. 128]. Такие перемены дают больше возможностей для противодействия киберпреступности, но вместе с тем ставят перед практикой и юридической наукой новые задачи.

Анализ следственной и оперативно-розыскной практики показывает, что преступники уже активно используют самые современные технологии в своих интересах. Речь идет не только о мессенджерах, инструментах для анонимности в сети и криптовалюте. По отдельности и в сочетании они и так сильно осложняют работу правоохранительных органов. Но кроме этого появляются и новые программные решения, которые все чаще применяют в преступной деятельности [1, с. 62].

По данным МВД России, в первом квартале 2025 г. более трети преступлений совершалось с использованием ИТТ, причем число таких деяний продолжало расти [4].

Законодатель отвечает на эту динамику последовательным расширением главы 28 УК РФ и дополняет ее составами, которые направлены против отдельных звеньев преступной инфраструктуры. В 2024–2025 гг. в главу включены ст. 272.1 о незаконном обороте компьютерной информации, содержащей персональные данные, и ст. 274.2–274.5, введенные Федеральным законом от 31.07.2025 N 282-ФЗ [9]. Федеральный закон от 26.07.2026 № 251-ФЗ дополнил главу ст. 274.6 и внес согласованные с ней изменения в ст. 31 и 151 УПК РФ о подсудности и подсудственности [10].

Закон № 251-ФЗ принимался на фоне перелома в динамике преступлений с использованием ИТТ. В первом квартале 2025 г. такие деяния прирастали быстрее общего массива преступности, а к концу года сокращались быстрее него [7]. Сильнее всего сократились собственно преступления в сфере компьютерной информации, слабее всего – мошенничества с использованием ИТТ. Для главы 28 УК РФ это различие существенно. Категория преступлений в сфере

компьютерной информации охватывает деяния, квалифицируемые по этой главе, тогда как номера и учетные записи, оборот которых запрещен ст. 274.4 и 274.5, служат прежде всего орудием мошенничеств и краж. Эффект новых составов уместно оценивать по динамике ИТТ-мошенничеств и дистанционных краж.

Число преступлений в сфере компьютерной информации сократилось почти в пять раз сильнее, чем число ИТТ-мошенничеств. Мошенничества с использованием ИТТ снизились лишь на 1,3 процентного пункта сильнее общего массива, тогда как дистанционные кражи – на 16,6 пункта. Именно в мошеннических схемах используются номера, оформленные на иностранцев и переданные третьим лицам [3]. Поэтому сокращение деяний, квалифицируемых по главе 28, не означает ослабления инфраструктуры мошенничества. Разрыв между двумя показателями и составляет криминологическое основание ст. 274.4–274.6.

В первом квартале наблюдался незначительный рост количества зарегистрированных в Российской Федерации преступлений на 0,6 %, и прирост ИТТ-преступлений превышал его в пять раз; по итогам года ИТТ-преступления сокращались на 4,5 процентного пункта быстрее общего массива [4; 7]. Основная часть сдвига пришлась на период до ноября (показатель за январь – ноябрь охватывает и преступления в сфере компьютерной информации). В сообщениях МВД России причины перелома не названы. Связывать его со ст. 274.3–274.5 преждевременно: эти составы введены Законом от 31.07.2025 № 282-ФЗ, то есть в середине отчетного года [9].

Относительная устойчивость ИТТ-мошенничеств при резком сокращении других видов киберпреступлений согласуется со смещением уголовно-правовых запретов к инфраструктуре мошенничества – номерам, SIM-картам и договорам связи с абонентами-иностранцами.

Новый состав, а именно ст. 274.6 УК РФ, касается уже не информации, а договоров связи. Нерешенным остается вопрос о том, охватывается ли такой состав родовым объектом главы 28, который был сформулирован при принятии УК РФ в 1996 г. применительно к безопасности компьютерной информации [8]. От ответа зависят квалификация, разграничение со смежными статьями о передаче абонентских номеров и о мошенничестве, а также оценка того, способен ли уголовно-правовой запрет сократить приток номеров в мошеннические схемы.

По изложению «Российской газеты», И. Игошин – первый зампред Государственной Думы по защите конкуренции, связывал принятие закона с тем, что огромное количество абонентских номеров, оформленных на иностранцев, оказывается в руках мошенников [3]. Прокуратура Томской области, разъясняя ст. 274.4 и 274.5 УК РФ, подчеркивает ограничительный признак: ответственность наступит только при совершении

указанных действий из корыстной заинтересованности либо в целях совершения иного преступления [5].

Статья 274.6 построена иначе и опирается на административную преюдицию. Доктринальная оценка такой конструкции в главе 28 пока не сложилась. Часть 1 ст. 272 УК РФ задает исходную модель главы и признает преступлением «неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации» [8]. Предметом здесь выступает сама информация, а вред выражается в изменении ее состояния или доступности. По той же модели построены ст.ст. 273 и 274 УК РФ о вредоносных программах и о нарушении правил эксплуатации средств хранения, обработки или передачи информации.

С 2025 г. глава пополняется составами иного рода: ст. 272.1 охраняет персональные данные, ст. 274.2–274.5 – средства связи и учетные записи, ст. 274.6 – порядок заключения договоров с абонентами-иностранцами [8].

Часть 1 ст. 274.4 УК РФ устанавливает ответственность за «организацию деятельности по передаче абонентских номеров... иным лицам в нарушение требований законодательства Российской Федерации», совершенную из корыстной заинтересованности либо в целях совершения иного преступления [8]. Санкция ч. 1 предусматривает штраф в размере до семисот тысяч рублей, принудительные работы либо лишение свободы на срок до трех лет. По разъяснению прокуратуры Томской области, ст. 274.4, 274.5 УК РФ не применяются при передаче абонентских номеров членам семьи, близким родственникам, иным лицам для получения ими услуг в личных целях [5]. Уголовно наказуемой, следовательно, становится лишь передача, связанная с последующим посягательством.

Статья 274.6 озаглавлена «Нарушение требований законодательства Российской Федерации при заключении договора об оказании услуг подвижной радиотелефонной связи с иностранным гражданином или лицом без гражданства» [8]. Нарушением признается неуказание идентификатора пользовательского оборудования либо заведомо недостоверный IMEI-код (IMEI – International Mobile Equipment Identity, международный идентификатор мобильного оборудования) [12].

Цель совершения иного преступления в ст. 274.6 не названа. Эта норма будет применяться при наличии судимости за аналогичное преступление либо факта привлечения к административной ответственности за аналогичное деяние два раза в течение года [10]. Криминализация опирается на повторность нарушения регулятивного требования, а не на опасность конкретного последствия.

Полагаем, что непосредственным объектом ст. 274.6 выступает установленный порядок

идентификации абонентов-иностранцев, а компьютерная информация затрагивается лишь опосредованно, через сведения базы данных оператора. Размещение состава в главе 28 объяснимо его системной связью со ст. 274.4: оба запрета направлены против номеров, выходящих из-под контроля оператора. Вместе с тем административно-преюдициальная конструкция сближает ст. 274.6 с нарушениями регулятивных правил. Для правоприменителя это означает иной предмет доказывания, поскольку связь договора с мошенничеством устанавливать не требуется, достаточно подтвердить заведомость и преюдицию.

Из данных составов только ст. 274.6 не содержит ни цели совершения иного преступления, ни корыстной заинтересованности, ни последствий. Она оказывается наиболее формальной в группе и меньше других зависит от доказывания умысла на последующее посягательство.

Регулятивной основой нового состава служит ст. 45.1 Федерального закона от 07.07.2003 № 126-ФЗ «О связи». Согласно которой договор с иностранным гражданином или лицом без гражданства должен содержать сведения о пользовательском оборудовании (об окончательном оборудовании), в том числе о его идентификаторе [11]. Оператор связи не вправе оказывать услуги подвижной радиотелефонной связи в случае использования идентификационного модуля в пользовательском оборудовании (оконечном оборудовании), сведения о котором отличаются от сведений, указанных в таком договоре.

Договор заключается при условии подтверждения достоверности сведений о таком лице с использованием единой системы идентификации и аутентификации и единой биометрической системы [11]. Требования адресованы оператору подвижной радиотелефонной связи и лицам, действующим от его имени; на договоры с гражданами Российской Федерации ст. 274.6 УК РФ не распространяется.

Субъектом ст. 274.6 на практике становится продавец сим-карты, оформляющий договор от имени оператора. Уголовная ответственность возникает только после двух административных наказаний в течение года либо при судимости за аналогичное преступление [10]. Максимальный штраф, согласно сообщениям о принятом законе, составляет 500 тыс. руб. С 6 августа 2026 года в России вступили в силу изменения в Уголовном кодексе, включая новую статью. Без преюдиции нарушение остается административным проступком.

Административная преюдиция сужает охват нормы: продавец, впервые оформивший даже значительное число договоров без идентификатора, отвечает лишь в административном порядке, если не доказаны признаки ст. 274.4 УК РФ или соучастия в мошенничестве.

Результативность ст. 274.6 зависит от того,

как быстро сведения об административных наказаниях продавцов становятся доступны органам расследования. Без такого обмена преюдиция не складывается. Второе условие – единообразное понимание заведомой недостоверности идентификатора. Этим условиям отвечают следующие меры: - учет операторами связи работников и агентов, привлеченных к административной ответственности за нарушение ст. 45.1 Закона «О связи», с передачей сведений в МВД России – это сократит срок формирования преюдиции; - Пленуму Верховного Суда РФ целесообразно разъяснить признак заведомой недостоверности идентификатора и соотношение ст. 274.6 и 274.4 УК РФ; - в статистической отчетности МВД России ст. 274.3–274.6 УК РФ нужны отдельные строки, позволяющие оценить применение каждого состава.

Если операторы обеспечат предусмотренный ст. 45.1 Закона «О связи» отказ в услугах при несовпадении идентификатора оборудования, уголовных дел по ст. 274.6 будет немного, а действие нормы окажется преимущественно превентивным. При слабом техническом контроле норма станет основным инструментом воздействия на розничное звено оборота номеров, и ее применение будет расти вслед за административной практикой.

Таким образом, мы видим, что статья 274.6 УК РФ завершает формирование в главе 28 группы составов, которые охраняют порядок оборота абонентских номеров и учетных данных и лишь опосредованно связаны с безопасностью ком-

пьютерной информации. Ее непосредственный объект – порядок идентификации абонентов-иностранцев. От ст. 274.2–274.5 новый состав отличается административной преюдицией и отсутствием цели совершения иного преступления, что делает его самым формальным в группе.

В 2025 г. преступления в сфере компьютерной информации сокращались значительно быстрее ИТТ-мошенничеств, и эта динамика согласуется со смещением уголовно-правовых запретов к инфраструктуре мошенничества.

Для практики значимы два следствия. Доказывание по ст. 274.6 сосредоточено на заведомости нарушения и наличии преюдиции; связь конкретного договора с мошенничеством устанавливать не нужно. Исключение дел из подсудности мировых судей переносит их рассмотрение в районные суды, а правила подсудности главы 28 распространяются на новый состав. Выводы о результативности нормы ограничены тем, что она действует с августа 2026 г. и практика ее применения еще не сложилась. Предложенные меры направлены на ускорение формирования преюдиции и на единообразие толкования признака заведомой недостоверности.

Дальнейшие исследования целесообразно направить на анализ первых приговоров по ст. 274.4–274.6 УК РФ и на соотношение этих составов со ст. 159 УК РФ. Отдельного изучения требует вопрос о выделении составов против порядка использования средств связи в самостоятельную главу Особенной части.

Список литературы:

- [1] Батоев, В.Б. О современном состоянии и противодействии преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий / В.Б. Батоев // ЮристыПравоведь. – 2023. – N 2(105). – С. 59-67.
- [2] Дашин А.В., Усенко А.С., Бузина А.Л. Преступления, совершаемые с использованием информационно-телекоммуникационных технологий: сущностная и атрибутивная характеристика // Вестник экономики и права. 2026. С. 127-134.
- [3] За нарушения при продаже сим-карт мигрантам накажут по УК // Российская газета. 2026. 8 июля. URL: <https://rg.ru/2026/07/08/za-narusheniia-pri-prodazhe-sim-kart-migrantam-nakazhut-po-uk.html> (дата обращения: 24.09.2026).
- [4] Краткая характеристика состояния преступности в Российской Федерации за январь – март 2025 года // Официальный сайт МВД России. URL: <https://xn-b1aew.xn-p1ai/reports/item/64450541/> (дата обращения: 24.09.2026).
- [5] Прокурор разъясняет // Официальный сайт прокуратуры Томской области. URL: https://epp.genproc.gov.ru/ru/proc_70/activity/legal-education/explain/e8313603/ (дата обращения: 24.09.2026).
- [6] Сердюкова Е.В., Чуниха А.А., Зиновьева Е.О. Особенности уголовной ответственности за преступления в сфере компьютерной информации // Восточно-европейский научный журнал. 2021. С. 57-59.
- [7] Статистические сведения о состоянии преступности в 2025 году // Официальный медиапортал МВД России. URL: <https://mvdmedia.ru/news/official/statisticheskie-svedeniya-o-sostoyanii-prestupnosti-v-2025-godu/> (дата обращения: 24.09.2026).
- [8] Уголовный кодекс Российской Федерации: фед. закон от 13.06.1996 № 63-ФЗ // СЗ РФ. - 1996. - № 25. - Ст. 2954.
- [9] Федеральный закон от 31.07.2025 №282-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» // СПС «КонсультантПлюс». URL: <https://www.consultant.ru/> (дата обращения 28.09.2026).
- [10] Федеральный закон № 251-ФЗ «О внесении изменений в Уголовный кодекс Российской Фе-

дерации и статьи 31 и 151 Уголовно-процессуального кодекса Российской Федерации» // СПС «КонсультантПлюс». URL: <https://www.consultant.ru/> (дата обращения 28.09.2026).

[11] Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» // СПС «КонсультантПлюс». URL: <https://www.consultant.ru/> (дата обращения 28.09.2026).

[12] IMEI // Рувики: Интернет- энциклопедия. URL: <https://clck.su/OjoAx> (дата обращения 28.09.2026).

References:

[1] Batoev, V.B. On the current state of and countermeasures against crimes committed using information and telecommunication technologies / V.B. Batoev // *Yurist-Pravoved*. – 2023. – No. 2(105). – P. 59-67.

[2] Dashin A.V., Usenko A.S., Buzina A.L. Crimes committed using information and telecommunication technologies: essential and attributive characteristics // *Bulletin of Economics and Law*. 2026. P. 127-134.

[3] Penalties under the Criminal Code for violations in the sale of SIM cards to migrants // *Rossiyskaya Gazeta*. 2026. July 8. URL: <https://rg.ru/2026/07/08/za-narusheniia-pri-prodazhe-sim-kart-migrantam-nakazhut-po-uk.html> (accessed: September 24, 2026).

[4] Brief overview of the crime situation in the Russian Federation for January–March 2025 // Official website of the Russian Interior Ministry. URL: <https://xn-b1aew.xn-p1ai/reports/item/64450541/> (accessed: September 24, 2026).

[5] Prosecutor's explanation // Official website of the Tomsk Region Prosecutor's Office. URL: https://epp.genproc.gov.ru/ru/proc_70/activity/legal-education/explain/e8313603/ (accessed: September 24, 2026).

[6] Serdyukova E.V., Chunikha A.A., Zinovyeva E.O. Specifics of criminal liability for crimes involving computer information // *East European Scientific Journal*. 2021. Pp. 57–59.

[7] Statistical data on the state of crime in 2025 // Official media portal of the Russian Ministry of Internal Affairs. URL: <https://mvdmedia.ru/news/official/statisticheskie-svedeniya-o-sostoyanii-prestupnosti-v-2025-godu/> (accessed: 24.09.2026).

[8] Criminal Code of the Russian Federation: Federal Law No. 63-FZ dated June 13, 1996 // *Collected Legislation of the Russian Federation*. 1996. No. 25. Art. 2954.

[9] Federal Law No. 282-FZ dated July 31, 2025, «On Amendments to Certain Legislative Acts of the Russian Federation» // *ConsultantPlus Legal Reference System*. URL: <https://www.consultant.ru/> (accessed: 28.09.2026).

[10] Federal Law No. 251-FZ «On Amendments to the Criminal Code of the Russian Federation and Articles 31 and 151 of the Criminal Procedure Code of the Russian Federation» // *ConsultantPlus Legal Reference System*. URL: <https://www.consultant.ru/> (accessed: 28.09.2026).

[11] Federal Law No. 126-FZ dated July 7, 2003, «On Communications» // *ConsultantPlus Legal Reference System*. URL: <https://www.consultant.ru/> (accessed: 28.09.2026). [12] IMEI // *Ruviki: Online Encyclopedia*. URL: <https://clck.su/OjoAx> (accessed September 28, 2026).

