

Второй пакет мер противодействия кибермошенничеству

Вниманию руководителей и сотрудников операторов связи, кредитных организаций, представителей делового сообщества, а также лиц, желающих защитить себя от мошенников

Юридическая компания «Пепеляев Групп» информирует о разработке Минцифры России Проекта закона, направленного на противодействие кибермошенничеству (далее – Проект закона).¹

Напомним, 1 апреля 2025 г. был принят Закон № 41-ФЗ², содержащий первый пакет мер по борьбе с кибермошенничеством³.

Текущий проект закона подготовлен в целях дальнейшего совершенствования регулирования противодействия кибермошенничеству, развивает механизмы, установленные Законом № 41-ФЗ, а также вводит дополнительные правовые меры защиты.

Вступление в силу нового законопроекта планируется 1 марта 2026 г., за исключением некоторых положений.

Также подготовлены два сопутствующих законопроекта, направленные на введение новых составов правонарушений в КоАП РФ и УК РФ, а также ужесточение ответственности по ряду уже действующих норм в области ИТ⁴.

Вступление в силу поправок в КОАП РФ планируется также 1 марта 2026 г. Дата вступления в силу поправок в УК РФ и УПК РФ проектом закона не определена, в связи с чем изменения будут действовать по истечении 10 дней со дня их официального опубликования.

¹ Проект закона «О внесении изменений в отдельные законодательные акты Российской Федерации (в части противодействия правонарушениям, совершаемым с использованием информационно-коммуникационных технологий)» // ID проекта: 159652

² Федеральный закон от 01.04.2025 № 41-ФЗ «О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации».

³ Подробнее см. здесь: <https://www.pgplaw.ru/analytics-and-brochures/alerts/vstupil-v-silu-zakon-o-protivodeystvii-kibermoshennichestvu/>.

⁴ Проект закона «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» // ID проекта: 159659 и проект закона «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации» // ID проекта: 159661

Государственная информационная система противодействия нарушениям (ГИС)

Расширение перечня информации, хранящейся в ГИС

В текущей редакции Закона № 41-ФЗ в ГИС хранится информация о лицах, совершивших противоправные действия, и об абонентских номерах, с применением которых были совершены противоправные действия.

Проектом закона предлагается реформировать ГИС: создать реестр абонентских номеров, в котором будут храниться информация о лицах-мошенниках, их абонентских номерах, абонентских номерах жертв мошенников, а также записи переговоров с признаками противоправных действий.

Вступление поправок в силу в этой части планируется с 1 января 2026 года.

Меры противодействия мошенничеству, связанные с деятельностью операторов связи

Создание баз данных идентификаторов пользовательского оборудования (оконечного оборудования)

Проектом закона предлагается создание двух баз данных идентификаторов (IMEI) мобильных устройств:

1. база данных IMEI, формируемая оператором связи при регистрации абонентского устройства для оказания услуг связи;
2. центральная база данных IMEI, находящаяся в ведении Минцифры России и содержащая разрешение/запрет на использование устройства. Предполагается, что источником формирования центральной базы данных будут базы данных операторов связи. Порядок их взаимодействия определит Минцифры. Требования к центральной базе данных будут установлены Правительством РФ.

Операторы связи будут предоставлять свои услуги только при использовании абонентом «разрешенного» устройства. В случае, если IMEI устройства отнесен к «неразрешенным», оператор связи будет обязан приостановить оказание услуг связи. К устройствам, не разрешенным для использования в сети связи, относятся устройства с IMEI:

- в отношении которых было принято решение о запрете;
- которые не соответствуют законодательным требованиям.

Требования к IMEI и порядок их отнесения к разрешенным или не разрешенным будут определены Минцифры России.

При этом программное изменение IMEI не допускается. Действия лица по «перепрошивке» IMEI телефона могут быть квалифицированы по ст. 13.6

КОАП РФ («Использование средств связи, не прошедших процедуру подтверждения их соответствия установленным требованиям») и повлечь наказание в виде конфискации устройства с наложением штрафа в размере до 5 тыс. руб. для физических лиц, до 30 тыс. руб. на должностных лиц, до 300 тыс. руб. на юрлиц.

Более того предлагается установить в качестве квалифицирующего признака двух составов преступлений, предусмотренных ч. 3 ст. 158 и ч. 3 ст. 159 УК РФ (кража и мошенничество) сокрытие информации о пользователе услуг связи (то есть изменение IMEI) с наказанием вплоть до 6 лет лишения свободы.

Вступление поправок в силу в этой части планируется 1 марта 2027 г.

Новые обязанности операторов связи при взаимодействии с ГИС

Операторы связи будут самостоятельно выявлять абонентские номера с признаками осуществления противоправных действий и передавать в ГИС сведения:

- об абонентском номере, с которого осуществляются противоправные действия;
- об абонентском номере потерпевшего лица;
- о месте нахождения устройства.

Порядок выявления признаков противоправных действий будет установлен Минцифры России при согласовании с ЦБ РФ.

При получении указания от ГИС оператор связи будет обязан приостановить оказание услуг абоненту на 24 часа.

По запросу Минцифры оператор связи обязан будет передать в ГИС записи телефонных разговоров, имеющих признаки противоправных действий.

Маркировка звонков

Проект закона уточняет нормы, обязывающие маркировать звонки от ИП и юрлиц.

Действующая редакция п. 9.1. ст. 46 Закона о связи возлагает соответствующие обязанности исключительно на операторов связи, и в законодательстве отсутствует прямой запрет на осуществление немаркированных вызовов, а к субъектам предпринимательской деятельности требования о маркировке не предъявляются.

В п. 9.1. ст. 46 Закона о связи предлагается установить условие о возможности вызова исключительно при передаче сведений о звонящем оператору связи принимающей стороны. В ст. 45 Закона о связи вводится норма, согласно которой инициирование телефонного вызова от ИП или

юрлица допускается только при условии обязательной передачи на устройство принимающего лица информации о звонящем.

Комментарий «Пепеляев Групп»

Требование маркировки звонков породило немало дискуссий еще с момента принятия первого пакета мер противодействия мошенничеству.

Во-первых, предусмотренная в Законе о связи обязанность для операторов связи маркировать звонки, не корреспондирует обязанности юрлиц и ИП сообщать, передавать операторам связи сведения, необходимые для маркировки. Это привело к тому, что операторы связи стали тем или иным способом стимулировать бизнес заключать с ними договоры, автоматически удерживая стоимость маркировки с корпоративных абонентов либо блокируя вызовы, квалифицируя их как «массовые». Учитывая, что в настоящее время критерия «массовости» не установлено, каждый оператор связи выработал свой подход.

Кроме того, операторы связи, беспокоясь о том, что не исполняют требования Закона о связи, заняли консервативную позицию и предложили бизнесу маркировать звонки со всех корпоративных номеров, даже если они используются только для внутрикорпоративной связи. И это вступает в противоречие с Постановлением Правительства РФ от 28.08.2025 № 1300, в котором к числу сведений, передаваемых операторам, относится перечень абонентских номеров, с которых будут осуществляться вызовы (т.е. не все абонентские номера).

На сегодняшний день отсутствует специальная (прямая) статья в КоАП РФ, предусматривающая ответственность для операторов связи за неисполнение требования о маркировке. Между тем, сохраняется риск применения такой крайней меры, как лишение лицензии за неисполнение ее условий, к числу которых относится исполнение требований Закона о связи, включая маркировку.

Также не исключена вероятность квалификации звонков без маркировки как массовых вызовов без согласия абонентов по п. 4.1. ст. 14.3 КоАП РФ («Нарушение требований к рекламе, распространяемой по сетям электросвязи»). По этой статье к ответственности может быть привлечено любое лицо. Напомним, штрафы по п. 4.1 ст. 14.3 КоАП РФ для ИП – от 20 тыс. руб. до 100 тыс. руб., для организаций – от 300 тыс. руб. до 1 млн. руб.

В таких условиях оператор связи блокирует вызовы, которые квалифицировал для себя как «массовые». А к таким могут быть отнесены и те вызовы, которые осуществляются с колл-центра компании, например, по претензиям покупателей.

«Самозапрет» на иностранные вызовы

Предлагается предоставить абонентам возможность установить «самозапрет» на получение звонков с иностранных номеров. Член Комитета Госдумы по информполитике Антон Горелкин отмечает, что мера схожа с «самозапретом» на кредиты и ее реализация будет возможна через «Госуслуги»⁵.

Ответственность операторов связи

1. Устанавливается ответственность операторов связи в случае неисполнения обязанностей при взаимодействии с ГИС.

Как указано выше, у операторов связи появятся новые обязанности по выявлению признаков правонарушений с использованием абонентских номеров, направлению указанной информации в ГИС и, в случае получения указания от ГИС, приостановления услуг связи. При ненадлежащем исполнении оператором связи своих обязанностей, которое повлекло хищение денежных средств с мобильного счета абонента, оператор связи обязан будет возместить абоненту ущерб.

2. Предлагается ввести новые составы правонарушений в КоАП РФ и УК РФ для операторов связи и их должностных лиц.

2.1. КоАП РФ:

- несоблюдение требований к количеству сим-карт, находящихся в пользовании одного физического лица;
- оказание услуг связи иностранному гражданину (лицу без гражданства) в случае использования им устройства, IMEI которого не включен в договор оказания услуг;
- нарушение порядка представления информации в государственную информационную систему мониторинга исполнения операторами связи обязанностей при оказании услуг связи либо нарушение требований законодательства по ее использованию.

2.2. При повторном нарушении требования о включении IMEI в договор оказания услуг связи, если такое нарушение повлекло причинение крупного ущерба, должностное лицо оператора связи понесет уголовную ответственность.

Иные меры противодействия кибермошенничеству, касающиеся деятельности операторов связи

1. Новые требования к использованию виртуальных телефонных станций (ВТС)

⁵ <https://realnoevremya.ru/news/353731-gosduma-predlozhit-rossiyanam-samozapret-na-inostrannye-zvonki>

Проектом закона устанавливаются новые требования к функционированию ВАТС.

При использовании сетевых адресов для взаимодействия с ВАТС такие адреса должны соответствовать российской национальной системе доменных имен. Дополнительно при привлечении услуг хостинг-провайдеров провайдеры должны быть включены в официальный реестр провайдеров хостинга, ведение которого осуществляет Роскомнадзор. Аналогичное требование предлагается закрепить в ст. 10.2-1 Закона о защите информации («Особенности регулирования деятельности провайдера хостинга»).

2. Расширение обязанностей операторов связи

Проект закона расширяет объем информации, передаваемой операторами связи в систему мониторинга.

Операторы будут обязаны предоставлять сведения об абонентских номерах, используемых в абонентских терминалах пропуска трафика (SIM-боксы), с указанием типа оборудования, идентификаторов радиоэлектронных средств, адресов установки и целей использования. Также в систему мониторинга должна передаваться информация об абонентских номерах ВАТС и сетевых адресах, используемых для предоставления услуг связи.

Меры противодействия мошенничеству, связанные с деятельностью кредитных организаций

Проектом закона предлагается внести изменения в Федеральный закон «О национальной платежной системе» в части регулирования деятельности кредитных организаций или операторов по переводу денежных средств (далее - ОПДС).

Новые полномочия и требования к ОПДС: усиление контроля за переводами без согласия клиента

1. Абонентские номера

Положения Проекта закона обязывают ОПДС получать сведения из ГИС при проверке добровольности переводов денежных средств клиентами:

- об абонентских номерах, через которые совершаются действия, имеющие признаки противоправных;
- об абонентских номерах, на которые совершаются действия (телефонные вызовы или короткие текстовые сообщения), имеющие признаки противоправных.

При наличии сведений о возможных противоправных действиях, связанных с абонентскими номерами клиентов, ОПДС будут вправе приостановить использование такими клиентами электронных средств платежа на период нахождения номера в едином реестре номеров,

используемых для противоправных действий. Порядок приостановления должен быть предусмотрен договором с клиентом.

В то же время, ОПДС будут обязаны самостоятельно направлять в ГИС сведения о таких абонентских номерах. Состав и порядок направления такой информации будет устанавливаться Банком России по согласованию с Минцифры России.

2. Вредоносное ПО

ОПДС будут обязаны использовать информацию о воздействии вредоносного кода на ПО, применяемое клиентами для переводов денежных средств.

При выявлении воздействия вредоносного кода ОПДС обязаны отказать в выполнении распоряжения клиента или совершении операции (перевода). Клиент незамедлительно уведомляется о причинах отказа. В таких случаях, клиент или его представитель могут совершить перевод только при личном присутствии у ОПДС.

Также ОПДС обязаны предусмотреть обеспечение защиты своего ПО (включая мобильные приложения и сайты), используемого клиентом, от воздействия вредоносного кода и выявлять случаи такого воздействия до списания средств клиента, включая операции с платежными картами, переводами электронных денег или через СБП.

Договор с клиентом должен содержать положения, позволяющие клиенту согласиться или отказаться от такой защиты.

Ответственность ОПДС за ненадлежащую проверку добровольности переводов

Согласно Проекту закона ОПДС исполнивший перевод или операцию, несмотря на полученные сведения о противоправных действиях, рискует понести негативные финансовые последствия: ОПДС будет обязан полностью возместить суммы перевода клиенту-физическому лицу при наличии постановления о возбуждении уголовного дела по факту хищения средств. Возмещение осуществляется не позднее 30 дней с момента получения обращения клиента.

Ограничение количества платежных карт

Проектом закона устанавливается ограничение на выдачу одному клиенту-физическому лицу:

- более 5 платежных карт одним ОПДС;
- более 10 платежных карт совокупно всеми российскими кредитными организациями и открытыми в России филиалами иностранных банков физическому лицу.

Совет директоров Банка России может увеличить данные лимиты.

Комментарий «Пепеляев Групп»

Проект закона умалчивает о том, что будет с платежными картами клиентов, у которых на 1 марта 2026 г. окажется более 5 платежных карт в одном или более 10 в разных ОПДС. Мы полагаем, что ограничение будет распространяться только на выдачу платежных карт после вступления закона в силу.

Меры противодействия мошенничеству в сфере информационной безопасности

Новые обязанности владельцев онлайн-платформ при взаимодействии с ГИС

Проект закона вводит обязанность для:

- организаторов сервисов обмена мгновенными сообщениями,
- провайдеров хостинга,
- владельцев социальных сетей,
- владельцев сервисов размещения объявлений

принимать меры, направленные на предотвращение и пресечение правонарушений, а также передавать в ГИС сведения о признаках совершения противоправных действий.

Перечень указанных мер и состав передаваемых сведений будет определен Правительством РФ.

Расширен перечень информации, доступ к которой подлежит ограничению

Проектом закона предлагается расширить перечень информации, распространяемой с нарушением закона и подлежащей ограничению. В частности, сюда относятся:

- информация, предназначенная для несанкционированного вмешательства в ПО или распространяющая вредоносные ПО;
- информация, направленная на введение в заблуждение. К ней относятся сообщения, выдаваемые за достоверные, но способные причинить имущественный ущерб пользователю либо принадлежащей ему информации. Подробные критерии такой информации будут установлены Правительством РФ.

Иные меры противодействия мошенничеству

Интеграция управления персональными данными с «Госуслугами»

Проектом закона предусмотрена возможность субъектов персональных данных (ПД) управлять своими ПД через сервис «Госуслуги». Субъект ПД будет вправе:

- дать свое согласие на обработку ПД через «Госуслуги» (типовая форма будет разработана Роскомнадзором);
- отозвать свое согласие на обработку ПД через «Госуслуги»;
- получить через «Госуслуги» информацию, подтверждающую факт обработки ПД;
- обжаловать действия оператора ПД в случае нарушения прав и свобод субъекта ПД.

При этом планируется обязать операторов при сборе ПД передавать в «Госуслуги» информацию о фактах обработки ПД. Операторы, которые осуществляли обработку ПД до дня вступления нормы в силу (до 01.03.2028), обязаны передать в «Госуслуги» данные сведения.

Вступление поправок в силу в этой части планируется 1 марта 2028 г.

Комментарий «Пепеляев Групп»

Предполагаемая поправка вызывает вопросы с точки зрения ее практической реализации.

Во-первых, требование передачи сведений о каждом факте обработки ПД при сборе ПД представляется избыточным. Оператор ПД может произвести несколько раз сбор ПД у одного и того же субъекта. Достаточно было бы ограничиться передачей сведений о получении согласия субъекта ПД – именно согласие определяет законность обработки.

Во-вторых, передача всех сведений об обработке ПД при их сборе до вступления нормы в силу труднореализуема. Оператор ПД не обязан фиксировать факты, связанные со сбором ПД (в отличие от получения согласия на обработку), в связи с чем не сможет передать соответствующие сведения.

Сертификаты безопасности национального удостоверяющего центра (НУЦ)

В числе готовящихся изменений планируется создание новой категории цифровых сертификатов – сертификатов безопасности НУЦ, выдаваемых через ГИС.

Сертификат безопасности НУЦ будет использоваться для:

- обеспечения устойчивого и защищенного взаимодействия с:
 - информационной системой;
 - сайтом в интернет-сети.
- аутентификации:
 - информационной системы;
 - сайта;
 - участника электронного взаимодействия в корпоративной системе.
- подтверждения:
 - владения информационной системой или сайтом;
 - целостности и подлинности происхождения программ для электронных вычислительных машин;
 - организации защищённого взаимодействия с участниками электронного обмена в корпоративных информационных системах.

Для госорганов обеспечение возможности взаимодействия через сертификаты безопасности НУЦ будет обязательным. В свою очередь, Правительство РФ вправе распространить данное требование и на других лиц.

Вступление поправок в силу в этой части планируется 1 июля 2026 г.

Установлен перечень способов восстановления доступа к аккаунту в «Госуслугах»

Согласно предлагаемым поправкам, в случае ограничения доступа лица к его аккаунту в «Госуслугах» в связи с выявлением факта получения несанкционированного доступа к аккаунту, восстановление возможно следующими способами:

- использование биометрии;
- посредством официального сайта банка или банковского приложения;
- в мессенджере «Мам»;
- посредством личной явки в центр «Госуслуг».

Ограничение на госрегистрацию прав недвижимости

Проект закона предусматривает поправки, согласно которым сроки осуществления государственного кадастрового учета и государственной регистрации прав в случае наличия признаков неравнозначного

встречного исполнения могут быть увеличены до 20 дней. Осуществление государственной регистрации прав на недвижимость приостанавливается в случае, если сделка содержит признаки сомнительной сделки, установленные Правительством РФ.

О чем подумать, что сделать

Операторам связи следует подготовиться к внедрению базы данных IMEI, обеспечению ее взаимодействия с центральной базой данных, интеграции с ГИС с учетом планируемых изменений, а также уведомить своих сотрудников об ужесточении ответственности за правонарушения в сфере связи.

Кредитным организациям важно пересмотреть системы мониторинга переводов и внедрить механизмы проверки добровольности операций с учетом данных из ГИС.

Операторам ПД необходимо собрать сведения о фактах обработки ПД и быть готовыми к их передаче в «Госуслуги».

Помощь консультанта

Специалисты «Пепеляев Групп» обладают значительным опытом в сфере консультирования операторов связи, кредитных и иных организаций по правовым вопросам.

Мы готовы оказать всестороннюю юридическую поддержку организациям при:

- определении рисков в случае принятия Проекта закона;
- подготовке правовых позиций по спорным вопросам, возникающим вследствие Проекта закона;
- разработке внутренних регламентов и процедур, необходимых для соблюдения планируемых к введению требований;
- представлении интересов в спорах с государственными органами.

Контактная информация



Наталья Коваленко
Партнер

T: +7 (495) 767 00 07
n.kovalenko@pgplaw.ru



Лидия Горшкова
Партнер

T: +7 (495) 767 00 07
l.gorshkova@pgplaw.ru