

COMPLIANCE-

ДАЙДЖЕСТ

Декабрь 2022



Compliance-дайджест: изменения законодательства в области ИБ за декабрь 2022 года

В новом выпуске нашего ежемесячного Compliance-дайджеста вас ждет подборка основных изменений законодательства в области кибербезопасности, произошедших в декабре прошлого года. Как изменились формы уведомлений в области обработки персональных данных, которые необходимо направлять в Роскомнадзор? Какие новшества появились в области защиты критической информационной инфраструктуры? Что должны уметь ИБ-специалисты в кредитно-финансовой сфере, согласно новому профстандарту? Какие нормативные правовые акты планирует разработать ФСТЭК России в 2023 году? Об этом и не только — в нашем дайджесте.

Персональные данные

1. Роскомнадзор подготовил изменения в форму проверочного листа, используемого ведомством при осуществлении государственного контроля за обработкой персональных данных. Соответствующий [проект ведомственного приказа](#) опубликован на федеральном портале нормативных правовых актов.

Поправки направлены на приведение списка контрольных вопросов в соответствие изменённым нормам 152-ФЗ, которые заработали с 1 сентября 2022 года. Список контрольных вопросов планируется изменить и дополнить в части выполнения требований по трансграничной передаче ПДн, уведомлению Роскомнадзора об инцидентах с ПДн, прекращению обработки ПДн, осуществлению блокирования и уничтожения ПДн. В случае принятия приказ вступит в силу с 1 марта 2023 года.

2. Роскомнадзору могут разрешить внепланово проверять соблюдение требований по обработке персональных данных аккредитованными ИТ-компаниями в случае выявления в интернете баз данных или их фрагментов с признаками принадлежности к таким организациям. [Проект постановления Правительства РФ](#) об этом опубликован на федеральном портале нормативных правовых актов.

3. Роскомнадзор своим [приказом № 180 от 28.10.2022](#) утвердил формы уведомлений о намерении осуществлять обработку персональных данных, об изменении сведений в ранее направленных уведомлениях и о прекращении обработки персональных данных.

На сайте ведомства размещены:

- [примеры заполнения новых форм уведомлений](#);
- [электронные формы новых уведомлений](#).

4. Роскомнадзор своим [приказом № 187 от 14.11.2022](#) утвердил порядок и условия взаимодействия ведомства с операторами в рамках ведения реестра учета инцидентов в области персональных данных.

5. Опубликован Федеральный закон [от 29.12.2022 № 572-ФЗ](#) «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации».

6. Опубликован [Федеральный закон от 29.12.2022 № 584-ФЗ](#) «О внесении изменений в Федеральный закон “Об информации, информационных технологиях и о защите информации”, который запрещает организациям с государственными участием и финансовым организациям передавать персональные данные граждан РФ через иностранные мессенджеры.

7. Минфин России представил для общественного обсуждения [проект приказа](#), содержащий условия и порядок обработки министерством персональных данных в рамках осуществления функций оператора государственной интегрированной информационной системы в сфере контроля за оборотом драгоценных металлов.

Государственные информационные системы

8. Правительство РФ утвердило положение о единой цифровой платформе «ГосТех». Соответствующее постановление об этом ([№ 2338 от 16.12.2022](#)) опубликовано на официальном интернет-портале правовой информации и вступило в силу **с 1 января 2023 года**.

Платформа предназначена для инфраструктурного, организационно-технологического и документационного обеспечения процессов жизненного цикла государственных информационных систем (ГИС). Функции оператора платформы будет выполнять Минцифры России. Также министерство может передать их государственному казенному учреждению.

Согласно постановлению, органы местного самоуправления, государственные (муниципальные) предприятия и учреждения, госкорпорации, госкомпании, публично-правовые компании, а также хозяйственные общества, более 50% в уставном капитале которых находится в государственной (муниципальной) собственности, вправе принять решение об использовании платформы «ГосТех» для реализации процессов жизненного цикла своих информационных систем.

Также документом внесены изменения в постановление Правительства РФ от 06.07.2015 № 676 в части применения итерационного подхода к разработке ГИС.

Критическая информационная инфраструктура

9. Правительство РФ своим постановлением [№ 2360 от 20.12.2022](#) приняло поправки в правила категорирования объектов КИИ и перечень показателей критериев значимости. Ряд изменений вступил в силу с **20 декабря 2022 года**. В частности, с этого момента ведомства разрешили привлекать к мониторингу актуальности и достоверности сведений об объектах КИИ подведомственные им организации. Мониторингу подлежат все сведения, указанные в [пункте 17 постановления Правительства РФ № 127 от 08.02.2018](#). Госорганы и российские юрлица могут подтверждать актуальность и достоверность сведений путем ознакомления с объектами КИИ по месту их нахождения. О выявленных в результате мониторинга нарушениях необходимо сообщать ФСТЭК России не позднее 30 дней со дня их обнаружения.

Ниже приведена таблица с перечнем измененных и новых показателей критериев значимости объектов КИИ и их значений.

Показатель		Значение показателя		
		III категория	II категория	I категория
I. Социальная значимость				
3.	Прекращение или нарушение функционирования объектов транспортной инфраструктуры, транспортных средств, в том числе высокоавтоматизированных транспортных средств, оцениваемые:			
	а) на территории, на которой возможно нарушение транспортного сообщения или предоставления транспортных услуг	в пределах территории 1 муниципального образования (численностью от 2 тыс. чел.) или 1 внутригородской территории города федерального значения	выход за пределы территории 1 муниципального образования (численностью от 2 тыс. чел.) или 1 внутригородской территории города федерального значения, но не за пределы территории 1 субъекта РФ или территории города федерального значения	выход за пределы территории 1 субъекта РФ или территории города федерального значения
	б) по количеству людей, для которых могут быть недоступны транспортные услуги (тыс. человек)	более или равно 2, но менее 1 000	более или равно 1 000, но менее 5 000	более или равно 5 000
5.	Отсутствие доступа к госуслуге, оцениваемое:			
	а) в максимальном допустимом времени, в течение которого	менее или равно 24, но более 12	менее или равно 12, но более 6	менее или равно 6

	госуслуга может быть недоступна для получателей такой услуги (часов)			
	б) во времени с момента приема запроса о предоставлении госуслуги органом, предоставляющим госуслугу, или подведомственной госоргану организацией, участвующей в предоставлении госуслуги, в течение которого госуслуга не может быть оказана (в процентах от времени предоставления услуги, предусмотренного административным регламентом)	менее или равно 30	более 30, но менее или равно 70	более 70
III. Экономическая значимость				
8.	Возникновение ущерба субъекту КИИ, который является госкорпорацией, государственным унитарным предприятием, госкомпанией, организацией ОПК, стратегическим акционерным обществом, стратегическим предприятием, оцениваемого в снижении уровня дохода (с учетом НДС, акцизов и иных обязательных платежей) по всем видам деятельности (процентов от годового объема доходов, усредненного за прошедший 5-летний период)	более или равно 1, но менее или равно 10	более 10, но менее или равно 20	более 20
9.	Возникновение ущерба бюджету РФ или субъекта РФ, оцениваемого в снижении выплат (отчислений) в соответствующий бюджет, осуществляемых субъектом КИИ (процентов прогнозируемого годового дохода федерального бюджета или бюджета субъекта РФ, усредненного за планируемый 3-летний период)	более 0,0003, но менее или равно 0,0006	более 0,0006, но менее или равно 0,001	более 0,001
10.	Прекращение или нарушение проведения клиентами операций по банковским счетам и (или) без открытия банковского счета или операций, осуществляемых субъектом КИИ, являющимся в соответствии с законодательством РФ системно значимой кредитной организацией, кредитной организацией, выполняющей функции оператора услуг платежной инфраструктуры системно значимых платежных	менее или равно 70	более 70, но менее или равно 120	более 120

	систем, кредитной организацией, значимой на рынке платежных услуг, оператором услуг платежной инфраструктуры, оказывающим услуги платежной инфраструктуры в рамках системно значимых платежных систем, оцениваемые средненежным (по отношению к числу календарных дней в году) количеством осуществляемых операций (млн единиц) (расчет осуществляется по итогам года, а для создаваемых объектов – на основе прогнозных значений)			
10.1	Прекращение или нарушение проведения операций по исполнению обязательств, осуществляемых субъектом КИИ, являющимся центральным контрагентом, средненежной размер обязательств которого по передаче денежных средств в валюте РФ по итогам клиринга за последние 12 месяцев (трлн руб.)	менее 1	более или равно 1, но менее 10	более или равно 10
10.2	Прекращение или нарушение проведения учетно-расчетных операций, осуществляемых субъектом КИИ, являющимся центральным депозитарием и регистратором финансовых транзакций, средненежное количество ценных бумаг (ISIN) российских эмитентов, которые учитывались на счетах в центральном депозитарии (оцениваемые за последние 12 месяцев в тыс. шт.)	менее 10	более или равно 10, но менее 25	более или равно 25
10.3	Прекращение или нарушение проведения операций по выплатам, передаче и размещению денежных средств, осуществляемых субъектом КИИ, являющимся НПФ, которые оцениваются суммой пенсионных накоплений и пенсионных резервов НПФ (млрд руб.)	более или равно 50, но менее 1 000	более или равно 1 000, но менее 2 000	более или равно 2 000
10.4	Прекращение или нарушение проведения операций по выплатам, перестрахованию, инвестициям, осуществляемых субъектом КИИ, являющимся страховой организацией, оцениваемые объемом активов (млрд руб.)	более или равно 100, но менее 1 500	более или равно 1 500, но менее 5 000	более или равно 5 000

10.5	Прекращение или нарушение выполнения функций по переводу денежных средств, осуществляемых субъектом КИИ, являющимся операторами услуг информационного обмена (некредитной организацией), который оценивается количеством заключенных договоров с кредитными организациями	более или равно 25, но менее 100	более или равно 100, но менее 150	более или равно 150
V. Значимость для обеспечения обороны страны, безопасности государства и правопорядка				
13.	Снижение показателей государственного оборонного заказа, выполняемого (обеспечиваемого) субъектом КИИ, оцениваемое:			
	а) в снижении объемов продукции (работ, услуг) в заданный период времени (процентов заданного объема продукции);	более 0, но менее или равно 10	более 10, но менее или равно 15	более 15
	б) в увеличении времени изготовления единицы продукции с заданным объемом (процентов установленного времени на изготовление единицы продукции)	более 0, но менее или равно 10	более 10, но менее или равно 40	более 40

Кроме того, с 21 марта 2023 года заработает еще одна новация, согласно которой в качестве исходных данных для категорирования будут использоваться перечни типовых отраслевых объектов КИИ. Формировать их смогут госорганы и российские юрлица, выполняющие функции по разработке, проведению или реализации госполитики и (или) нормативно-правовому регулированию в установленной сфере деятельности.

10. В России ввели административную ответственность за предоставление недостоверных сведений ФСТЭК России о результатах категорирования объектов КИИ. Соответствующий федеральный закон ([№ 518-ФЗ от 19.12.2022](#)) опубликован на официальном интернет-портале правовой информации.

Размер штрафов аналогичен наказанию за непредставление или несвоевременную подачу данных регулятору: для должностных лиц он составляет от 10 до 50 тысяч рублей, для юрлиц — от 50 до 100 тысяч рублей. Также введены административные штрафы за повторные нарушения. Должностным лицам в этом случае придется заплатить от 50 до 100 тысяч рублей, юридическим лицам — от 100 до 200 тысяч рублей.

11. ФСБ России своим приказом [№ 543 от 01.11.2022](#) утвердила трехлетний переходный период, в течение которого допускается осуществлять мероприятия по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты в интересах субъектов КИИ на основании заключенных с НКЦКИ соглашений о сотрудничестве. По истечении этого периода, согласно Указу Президента РФ от 1 мая 2022 г. № 250, для проведения таких работ организации смогут подключать только аккредитованные центры ГосСОПКА.

Предполагается, что за время переходного периода регулятор разработает необходимую нормативную правовую базу и проведет аккредитацию центров ГосСОПКА.

12. Президент России своим указом [№ 954 от 26.12.2022](#) включил в состав Межведомственной комиссии Совета Безопасности РФ по вопросам обеспечения технологического суверенитета государства в сфере развития критической информационной инфраструктуры РФ Президента Российской академии наук.

Лицензирование деятельности

13. ФСТЭК России представила для общественного обсуждения проекты ведомственных приказов об утверждении порядка лицензирования следующих видов деятельности:

- [по разработке и производству средств защиты конфиденциальной информации;](#)
- [по технической защите конфиденциальной информации.](#)

14. ФСТЭК России представила для общественного обсуждения проекты приказов об утверждении форм документов, используемых ведомством в процессе лицензирования следующих видов деятельности:

- [по разработке и производству средств защиты конфиденциальной информации;](#)
- [по технической защите конфиденциальной информации.](#)

15. ФСТЭК России утвердила требования по безопасности информации к средствам контейнеризации. [Информационное сообщение](#) регулятора об этом и [выписка](#) из требований опубликованы на сайте ведомства.

Регулятор определил минимально необходимые требования по безопасности информации, предъявляемые к:

- уровню доверия средства контейнеризации;
- хостовой операционной системе, в среде которой функционирует средство контейнеризации;
- составу функций безопасности средства контейнеризации;
- изоляции контейнеров;
- выявлению уязвимостей в образах контейнеров;
- проверке корректности конфигурации контейнеров;
- контролю целостности контейнеров и их образов;
- регистрации событий безопасности;
- управлению доступом;
- идентификации и аутентификации пользователей;
- централизованному управлению образами контейнеров и контейнерами в средстве контейнеризации.

Для дифференциации требований по безопасности информации к средствам контейнеризации устанавливается шесть классов защиты. Самый низкий класс – шестой, самый высокий – первый.

Новости в области стандартизации

16. Минтруд России своим приказом [№ 739н от 28.11.2022](#) утвердил профессиональный стандарт «Специалист по информационной безопасности в кредитно-финансовой сфере».

В стандарте описаны трудовые функции специалиста:

- обеспечение функционирования систем и средств защиты информации в организациях кредитно-финансовой сферы (КФС);
- управление инцидентами информационной безопасности в организациях КФС;
- аналитическое и организационное сопровождение деятельности по управлению рисками информационной безопасности в организациях КФС;
- методологическое обеспечение процессов информационной безопасности в организациях КФС;
- контроль обеспечения информационной безопасности и обеспечение операционной надежности (киберустойчивости) в организациях КФС;
- организация процессов обеспечения информационной безопасности в организациях КФС.

17. Представлены официальные тексты национальных стандартов РФ по управлению компьютерными инцидентами, ориентированные на субъектов КИИ:

- [ГОСТ Р 59709-2022 «Защита информации. Управление компьютерными инцидентами. Термины и определения»;](#)
- [ГОСТ Р 59710-2022 «Защита информации. Управление компьютерными инцидентами. Общие положения»;](#)
- [ГОСТ Р 59711-2022 «Защита информации. Управление компьютерными инцидентами. Организация деятельности по управлению компьютерными инцидентами»;](#)
- [ГОСТ Р 59712-2022 «Защита информации. Управление компьютерными инцидентами. Руководство по реагированию на компьютерные инциденты».](#)

Стандарты вступают в силу с **1 февраля 2023 года**.

18. Технический комитет по стандартизации «Криптографическая защита информации» подготовил проекты рекомендаций по стандартизации в области криптографии:

- Рекомендации по стандартизации [«Информационная технология. Криптографическая защита информации. Использование российских криптографических алгоритмов в протоколе обмена ключами в сети Интернет версии 2 \(IKEv2\)»;](#)
- Рекомендации по стандартизации [«ИТ.КЗИ. Криптографические алгоритмы выработки ключей шифрования информации и аутентификационных векторов, предназначенные для реализации в аппаратных модулях доверия для использования в подвижной радиотелефонной связи».](#)

Отраслевые изменения

19. Правительство РФ своим распоряжением [№ 4088-р от 22.12.2022](#) утвердило Концепцию формирования и развития культуры информационной безопасности граждан России. Её реализацию поручено обеспечить Минцифры России совместно с другими заинтересованными федеральными органами исполнительной власти. Исполнительным органам субъектов РФ рекомендуется учитывать положения Концепции при формировании и осуществлении региональных программ в сфере ИБ.

20. Официально опубликовано постановление Правительства РФ [от 08.12.2022 № 2250](#) «О внесении изменения в Положение о защите информации в платежной системе».

21. Опубликован приказ Главного управления специальных программ Президента РФ от 22.10.2022 № 163, устанавливающий перечень информации об отнесенных к ведению Главного управления специальных программ Президента РФ пунктах управления государством и Вооруженными Силами РФ, иных специальных объектах мобилизационного назначения и объектах их инфраструктуры, составляющей профессиональную тайну, а также требования к защите данной информации.

Финансовый сектор

22. Утверждены национальные стандарты РФ, разработанные Техническим комитетом № 122:

- [ГОСТ Р 57580.4-2022](#) «Безопасность финансовых (банковских) операций. Обеспечение операционной надежности. Базовый состав организационных и технических мер».
- [ГОСТ Р 57580.3-2022](#) «Безопасность финансовых (банковских) операций. Управление риском реализации информационных угроз и обеспечение операционной надежности. Общие положения».

ГОСТ Р 57580.4-2022 устанавливает требования к составу и содержанию мер обеспечения операционной надежности для тех уровней защиты, которые применяют финансовые организации при определении базового состава таких мер. Положения стандарта предназначены для использования кредитными организациями и некредитными финансовыми организациями, указанными в части первой статьи 76.1 Федерального закона № 86 от 10.07.2002 «О Центральном банке РФ».

ГОСТ Р 57580.3-2022 определяет требования к составу и содержанию мер по управлению риском реализации информационных угроз для уровней защиты, которые применяются финансовыми организациями в рамках планирования, реализации, контроля и совершенствования системы управления таким риском, а также систем управления, определенных в рамках семейств стандартов ОН и ЗИ комплекса стандартов.

Оба стандарта вступят в силу с 1 февраля 2023 года.

23. Подкомитет № 1 «Безопасность финансовых (банковских) операций» Технического комитета № 122 «Стандарты финансовых операций» [сообщил о новостях за 4 квартал 2022 года](#).

Согласно информационному сообщению, редакция проекта стандарта Банка России «Безопасность финансовых (банковских) операций. Обеспечение безопасности финансовых сервисов с использованием технологии цифровых отпечатков устройств» одобрена и готовится к утверждению и введению в действие в установленном Банком России порядке.

Кроме того, эксперты Рабочей группы 1 «Технологии формирования среды доверия в безопасности» подготовили проект стандарта Банка России СТО БР БФБО-1.8-2023 «Безопасность финансовых (банковских) операций. Обеспечение безопасности финансовых сервисов при проведении дистанционной идентификации и аутентификации. Состав мер защиты информации». Пока проект проходит обсуждение в Рабочей группе 1.

Продолжается разработка следующих национальных стандартов методической базы для работ по оценке соответствия и стандарта обеспечения безопасности при привлечении финансовыми организациями услуг аутсорсинга:

- ГОСТ Р (проект) «Безопасность финансовых (банковских) операций. Управление риском реализации информационных угроз и обеспечение операционной надежности. Методика оценки зрелости»;
- ГОСТ Р (проект) «Безопасность финансовых (банковских) операций. Обеспечение операционной надежности. Методика оценки соответствия»;
- ГОСТ Р (проект) «Безопасность финансовых (банковских) операций. Управление риском реализации информационных угроз и обеспечение операционной надежности. Базовый состав организационных и технических мер при аутсорсинге информационных технологий и использовании облачных услуг».

В 2023 году подкомитет планирует разработать следующие национальные стандарты:

- «Безопасность финансовых (банковских) операций. Управление риском реализации информационных угроз и обеспечение операционной надежности. Методика оценки соответствия»;
- «Безопасность финансовых (банковских) операций. Обеспечение операционной надежности. Методика оценки соответствия»;
- «Безопасность финансовых (банковских) операций. Управление риском реализации информационных угроз и обеспечение операционной надежности. Базовый состав организационных и технических мер при аутсорсинге информационных технологий и использовании облачных услуг».

Планы ФСТЭК на 2023 год

24. ФСТЭК России представила [План разработки нормативных правовых актов на 2023 год](#). Некоторые документы, планируемые к разработке:

- Проект указа Президента РФ «Об утверждении Положения о государственной системе защиты информации в РФ»;
- Проект приказа ФСТЭК России «Об утверждении Порядка осуществления ФСТЭК России лицензирования деятельности по технической защите конфиденциальной информации и о признании утратившим силу приказа ФСТЭК России от 17 июля 2017 г. № 134 "Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации"»;
- Проект приказа ФСТЭК России «Об утверждении Порядка осуществления ФСТЭК России лицензирования деятельности по разработке и производству средств защиты конфиденциальной информации и о признании утратившим силу приказа ФСТЭК России от 17 июля 2017 г. № 133 "Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации"»;
- Проект приказа ФСТЭК России «Об утверждении Порядка аттестации экспертов органов по сертификации и специалистов испытательных лабораторий»;

- Проект приказа ФСТЭК России «Об утверждении Порядка проведения проверки соблюдения лицензионных требований лицензиатами, осуществляющими деятельность по разработке и производству средств защиты конфиденциальной информации и о признании утратившим силу приказа ФСТЭК России от 20 июля 2012 г. № 90 "Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по исполнению государственной функции по контролю за соблюдением лицензионных требований при осуществлении деятельности по разработке и производству средств защиты конфиденциальной информации"»;
- Проект приказа ФСТЭК России «Об утверждении Порядка организации и осуществления Федеральной службой по техническому и экспортному контролю федерального государственного контроля за обеспечением защиты государственной тайны»;
- Проект приказа ФСТЭК России «Об утверждении Порядка проведения сертификации процессов безопасной разработки программного обеспечения средств защиты информации».

Автор дайджеста: Екатерина Борисенкова, консультант по информационной безопасности отдела комплаенс и аттестации центра «Solar Интеграция» компании «РТК-Солар»