2025-2026. Изменения требований в части проектирования, создания и эксплуатации информационных систем

Спиридонова Елена

Специалист аналитического отдела

инфотекс ТЕХНОДЕСТ

Белый поток

Тенденции 2022-2026 годов

создание условий для обеспечения технологической независимости, импортозамещения и усиления ИБ РФ

совершенствование нормативной базы с акцентом на обеспечение принципов практической безопасности

последовательное ужесточение ответственности и усиление контроля государства за нарушениями требований ИБ

Направления деятельности

- Государственные информационные системы
- Критическая информационная инфраструктура
- Доверенные ПАКи/Импортозамещение
- Лицензирование и сертификация
- Защита гос. тайны и конфиденциальной информации
- Безопасное программное обеспечение
- ГосСОПКА
- Персональные данные

Указ Президента РФ от 30.03.2022 №166
«О мерах по обеспечению технологической независимости и безопасности КИИ РФ»

Указ Президента РФ от 01.05.2022 №250
«О дополнительных мерах по обеспечению ИБ РФ»

инфотекс

- с 31 марта 2022 года заказчикам **ЗАПРЕЩЕНО** без согласования с уполномоченным ФОИВ осуществлять закупки иностранного ПО (в том числе в составе ПАК) и услуг в целях использования на ЗО КИИ РФ
- с 1 сентября 2024 года **ЗАПРЕЩЕНО** использование субъектами КИИ РФ на принадлежащих им ЗО КИИ РФ ПАК, приобретенных … с 1 сентября 2024 года и не являющихся доверенными ПАК, за исключением случаев отсутствия … доверенных ПАК, являющихся аналогами приобретенных субъектами КИИ РФ ПАК…
- с 1 января 2025 года **ЗАПРЕЩЕНО** использовать иностранное ПО на принадлежащих гос. органам ЗО КИИ, если иное не установлено ФЗ
- с 1 января 2025 года **ЗАПРЕЩЕНО** использовать СЗИ, происходящие из недружественных стран, а также пользоваться сервисами (работами, услугами) по обеспечению ИБ, предоставляемыми (выполняемыми, оказываемыми) этими организациями
- **ПЕРЕХОД НА** преимущественное **ПРИМЕНЕНИЕ ДОВЕРЕННЫХ ПАК НА ЗО КИИ** осуществляется до 1 января 2030 года …

Гос. информационные системы

Приказ ФСБ России от 18.03.2025 №117

«Об утверждении Требований о ЗИ, содержащейся в ГИС, иных ИС гос. органов, ГУП, гос. учреждений, с использованием шифровальных (криптографических) средств»

Вступил в силу 06.04.2025

Устанавливает:

- Сферу действия (расширена относительно 524 приказа)
- Критерии обязательности применения СКЗИ в ИС
- Порядок определения требуемого класса СКЗИ

Уровень значимости информации	Масштаб ИС (сегмента ИС)		
	ИС (сегмент), предназначенная для решения задач ИС на всей территории РФ или в пределах 2-х и более субъектов РФ	ИС (сегмент), предназначенная для решения задач ИС на всей территории РФ или в пределах 1-ого субъекта РФ	ИС (сегмент), предназначенная для решения задач ИС в пределах объекта(ов) одного гос. органа, муниципал. обр. и/или организации
Высокий	КВ	КС3	КС2
Средний	КС3	КС3	КС1
Низкий	КС2	КС1	КС1

Приказ ФСТЭК России от 11.04.2025 №117

«Об утверждении Требований о ЗИ, содержащейся в ГИС, иных ИС гос. органов, ГУП, гос. учреждений»

Вступил в силу 01.03.2026

Устанавливает:

- Сферу действия (расширена относительно 17 приказа)
- Требования по выполнению обновленных требований ФСБ России к использованию СКЗИ в ИС
- Новые правила определения масштаба ИС и возможные последствия для классов защищенности
- Требования к защите ИС ЗО КИИ
- Разработку и периодическую актуализацию единой политики ЗИ
- Требования к организации удаленного доступа сотрудников к внутренним ресурсам организации
- Применение ИИ в ИБ
- Требования к разработке безопасного ПО

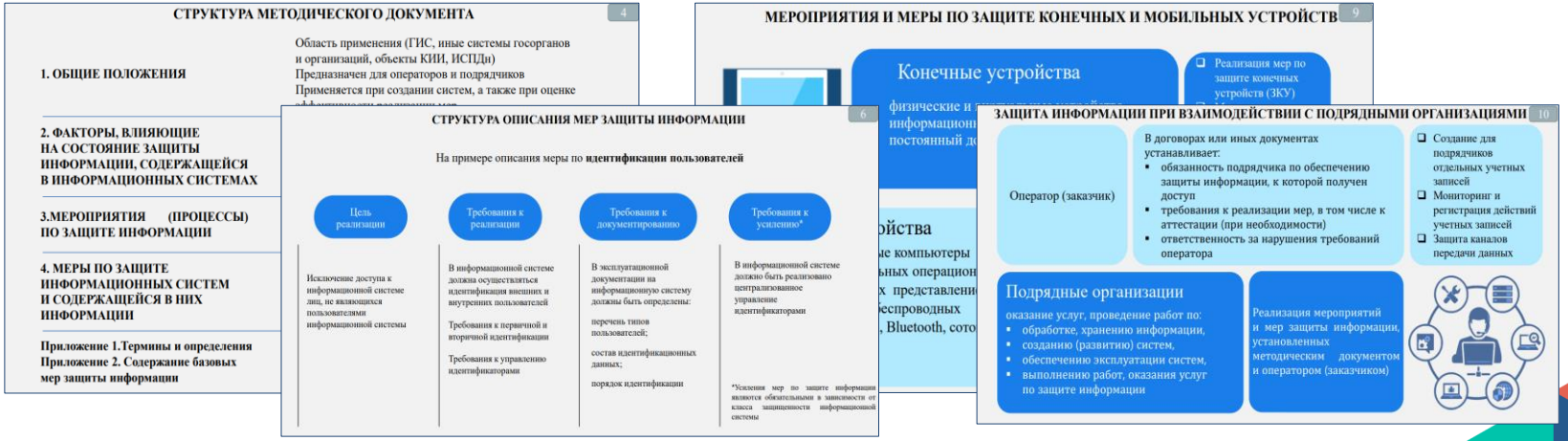
*Аттестованные на соответствие требованиям 17 приказа ФСТЭК России ИС переаттестации не подлежат**

ФСТЭК России. Мероприятия и меры по ЗИ в ИС

Проект Методического документа ФСТЭК России

«Мероприятия и меры по защите информации, содержащейся в информационных системах»

Утвержден ФТСЭК России 14.04.2026



По материалам И.С. Гефнер (ТБ Форум 2026)

Изменения в ФЗ «О безопасности КИИ РФ»

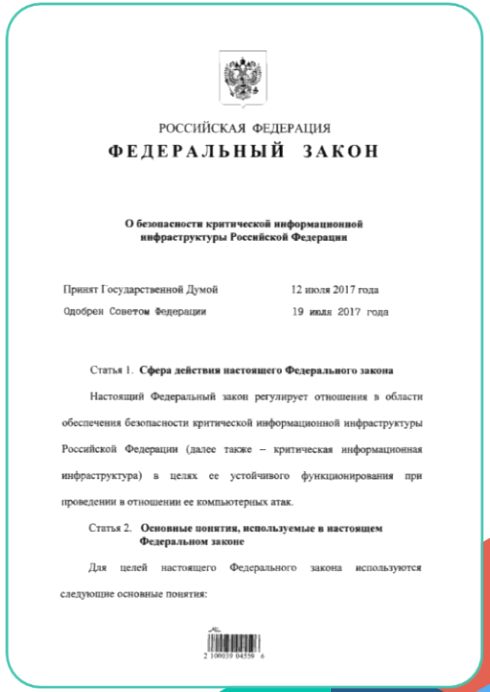
Федеральный закон от 07.04.2025 N 58-ФЗ
«О внесении изменений в ФЗ «О безопасности КИИ РФ»

Вступил в силу с 01.09.2025

Закреплена обязанность субъектов КИИ, которым принадлежат ЗО КИИ, использовать на таких объектах ПО, сведения о котором включены в Реестр ПО Минцифры

Правительство определяет:

- перечни типовых отраслевых объектов КИИ
  (Распоряжение Правительства РФ от 26.02.2026 №360-р)
- отраслевые особенности категорирования объектов КИИ
  (утверждены постановления Правительства для 5-ти сфер)
- требования к используемым на ЗО КИИ программно-аппаратным средствам
- порядок и сроки перехода субъектов КИИ на использование российского ПО
  (проект постановления Правительства РФ №159943. Завершено обсуждение)
- порядок осуществления мониторинга за исполнением субъектами КИИ обязанности по использованию на ЗО КИИ ПО, указанного в п.5 ч.3 статьи 9 187-ФЗ
  (проект постановления Правительства РФ №159847. Завершено обсуждение)
- …



РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНЫЙ ЗАКОН

О безопасности критической информационной инфраструктуры Российской Федерации

Принят Государственной Думой 12 июля 2017 года

Одобрен Советом Федерации 19 июля 2017 года

Статья 1. **Сфера действия настоящего Федерального закона**

Настоящий Федеральный закон регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации (далее также – критическая информационная инфраструктура) в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.

Статья 2. **Основные понятия, используемые в настоящем Федеральном законе**

Для целей настоящего Федерального закона используются следующие основные понятия:

Изменения в категорировании ЗО КИИ

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

Постановление Правительства РФ от 07.11.2025 № 1762

«О внесении изменений в ПП РФ от 08.02.2018 года № 127 «Об утверждении Правил категорирования объектов КИИ РФ, а также перечня показателей критериев значимости объектов КИИ РФ и их значений»

Вступило в силу с 17.11.2025

Согласно изменениям:

- установление соответствия объекта КИИ критериям значимости, расчет значений показателей критериев значимости и присвоение объекту КИИ одной из категорий значимости должны осуществляться **в соответствии с отраслевыми особенностями категорирования объектов КИИ**
- перечень сведений, который направляется в ФСТЭК России по результатам категорирования, дополняется доменными именами и сетевыми адресами объекта КИИ, взаимодействующего с сетями электросвязи общего пользования, в том числе с сетью «Интернет»

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

Распоряжение Правительства РФ от 26.02.2026 №360-р

«Об утверждении Перечня типовых отраслевых объектов критической информационной инфраструктуры РФ»

Вступило в силу с 26.02.2026

Для каждой из 14 сфер КИИ в ПП представлены типовые объекты (ИС, ИТКС, АСУ), типовые процессы, выполняемые объектом, и виды деятельности субъекта, для обеспечения которых используется типовой объект

Изменения в приказы ФСТЭК России 235 и 239

Проект приказа ФСТЭК России

«О внесении изменений в приказы ФСТЭК России от 21.12.2017 г. № 235 и от 25.12.2017 г. № 239»

Опубликован 07.04.2026

Изменения в 235 приказ

В рамках контроля состояния безопасности ЗО КИИ должен проводиться расчет и оценка:

- **показателя защищенности (Кзи)**
- **показатель уровня зрелости (Пзи)**

Расчет и оценка Кзи - не реже 1 раза в 6 месяцев.

Расчет и оценка Пзи - не реже 1 раза в 2 года.

Если значения Кзи и Пзи не соответствуют значениям, указанным в методиках ФСТЭК в течение 3 к.д. нужно проинформировать руководителя субъекта КИИ для принятия решения о проведении доп. мероприятий по ОБ ЗО КИИ.

Результаты оценки в срок не позднее 5 р.д. со дня их расчета направляются субъектом КИИ в ФСТЭК России для:

- мониторинга текущего состояния ОБ ЗО КИИ
- оценки эффективности деятельности по ОБ ЗО КИИ

Изменения в 239 приказ

Требования по обеспечению тех. поддержки СЗИ со стороны разработчиков (производителей). При её отсутствии на ЗО КИИ должны быть реализованы компенсирующие орг. и тех. меры

Прямой запрет лицам не являющимся работниками субъекта КИИ:

- **удаленного доступа** к ПО и ПАК ЗО КИИ, в том числе СЗИ, для обновления или управления
- **локального бесконтрольного доступа** к ПО и ПАК, в том числе СЗИ, для обновления или управления

Прямой запрет бесконтрольной передачи информации, в том числе технологической, разработчику (производителю) ПО и ПАК, или иным лицам.

Для **ЗО КИИ 1 и 2 категорий значимости** ПО и ПАК, **должны размещаться на территории РФ** за исключением случаев, когда установленных законодательством РФ и (или) международными договорами РФ

Исполнение ФЗ «О безопасности КИИ РФ»

Проект постановления Правительства РФ
«О порядке и сроках перехода субъектов КИИ РФ на использование программ для ЭВМ и БД, сведения о которых включены в единый реестр российских программ для ЭВМ и БД, предусмотренный статьей 12[1] ФЗ №149…»

Проектом устанавливаются:

- Сроки перехода – до 01.01.2028
  (в отдельных случаях до 01.12.2030)
- Правила перехода
- Ответственные за организацию перехода ФОИВ и организации

Проект постановления Правительства РФ
«Об утверждении Правил осуществления мониторинга за исполнением субъектами КИИ РФ обязанности по использованию на ЗО КИИ РФ программ для ЭВМ и БД, указанных в пункте 5 части 3 статьи 9 ФЗ «О безопасности КИИ РФ»

Проектом устанавливаются:

- Порядок осуществления мониторинга
- ФОИВ и организации, осуществляющие мониторинг

Исполнение ФЗ «О безопасности КИИ» (ФСБ России)

1. **Приказ ФСБ России от 23.12.2025 №539**
   «Об утверждении Порядка получения субъектами КИИ РФ информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения»
2. **Приказ ФСБ России от 24.12.2025 №540**
   «О внесении изменений в Положение о НКЦКИ, утвержденное приказом ФСБ России от 24.07.2018 г. № 366»
3. **Приказ ФСБ России от 25.12.2025 №546**
   «Об утверждении Порядка обмена информацией о компьютерных атаках и компьютерных инцидентах между субъектами КИИ РФ, между субъектами КИИ РФ и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты»
4. **Приказ ФСБ России от 25.12.2025 №547**
   «Об утверждении Порядка информирования ФСБ России о компьютерных атаках и компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов КИИ РФ и иных информационных ресурсов РФ, принадлежащих органам и организациям, на которые возложены обязанности, предусмотренные частью 4 статьи 9, 187-ФЗ …»
5. **Приказ ФСБ России от 25.12.2025 №548**
   «Об утверждении Порядка осуществления непрерывного взаимодействия субъектов КИИ РФ, которым на праве собственности, аренды или ином законном основании принадлежат ЗО КИИ РФ, а также руководителей органов и организаций, на которых возложены обязанности, предусмотренные частью 4 статьи 9, 187-ФЗ …, с ГосСОПКА»
6. **Приказ ФСБ России от 26.12.2025 №553**
   «Об утверждении Порядка и ТУ установки и эксплуатации средств, предназначенных для ОПЛПКА и реагирования на компьютерные инциденты, в том числе средств, предназначенных для поиска признаков компьютерных атак, за исключением средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов КИИ РФ»
7. **Приказ ФСБ России от 26.12.2025 №554**
   «Об установлении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, в том числе к средствам, предназначенным для поиска признаков компьютерных атак»

Доверенный ПАК

Указ Президента РФ № 166 от 30.03.2022
«О мерах по обеспечению технологической независимости и безопасности КИИ РФ»

«… определить сроки и порядок перехода субъектов КИИ на преимущественное применение доверенных программно-аппаратных комплексов …» (п.2, п.6)

Постановление Правительства РФ № 1912 от 14.11.2023
«О порядке перехода субъектов КИИ РФ на преимущественное применение доверенных ПАК … »

Пункт 2:

- ***Переход** на преимущественное применение доверенных ПАК на ЗО КИИ **осуществляется до 1 января 2030 года** …*
- ***с 1 сентября 2024 года не допускается использование субъектами КИИ РФ** на принадлежащих им ЗО КИИ РФ ПАК, **приобретенных … с 1 сентября 2024 года и не являющихся доверенными ПАК**, за исключением случаев отсутствия … доверенных ПАК, являющихся аналогами приобретенных субъектами КИИ РФ ПАК…*

Критерии признания ПАК доверенным

1. Сведения о ПАК содержатся в Реестре Минпромторга России
2. ПО, используемое в составе ПАК, включено в Реестр Минцифры России
3. ПАК, в случае реализации в нем функции защиты информации, сертифицирован ФСБ России и (или) ФСТЭК России

Обеспечение доверия к ПАК СЗИ ViPNet производства ИнфоТеКС

№	Требование к доверенным ПАК	Показатель выполнения
1	Сведения о ПАК ViPNet в Реестре Минпромторга России	53 **реестровые записи**
2	ПО, используемое в составе ПАК ViPNet, в Реестре Минцифры России	61 **реестровая запись**
3	Наличие действующих сертификатов соответствия ФСБ России для ПАК ViPNet	66 **сертификатов**
	Наличие действующих сертификатов соответствия ФСТЭК России для ПАК ViPNet	5 **сертификатов**

Порядка 60 ПАК ViPNet сегодня полностью удовлетворяют требованиям и могут быть признаны доверенными

Доверенный ПАК. Изменения

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

Проект постановления Правительства РФ
«О внесении изменений в постановление Правительства РФ от 14.11.2023 г. № 1912»

Опубликован 15.12.2025

Проектом предусмотрены следующие изменения:

Пункт 2:

С 1 января 2030 г. не допускается использование субъектами КИИ РФ на принадлежащих им ЗО КИИ РФ ПАК, не являющихся доверенными ПАК, за исключением следующих случаев:

- наличие заключенного договора удовлетворяющего требованиям…
- истечения срока полезного использования после 1 января 2030 г.
- функционирования ПАК на опасном производственном объекте, обеспечивающем выполнение работ, приостановка которых невозможна по производственно-техническим и технологическим условиям
- неотделимости ПАК от объекта капитального строительства

При условии обеспечения в отношении недоверенных ПАК, орг. и тех. мер защищенности КИИ РФ, решения о необходимости осуществления которых принимаются и направляются ФСБ России и ФСТЭК России

Критерии признания ПАК доверенным

1. Сведения о ПАК **или обо всех используемых в составе ПАК ПАС** содержатся в Реестре Минпромторга России
2. ПО, используемое в составе ПАК **и/или** ПАС, включено в **Реестр Минцифры России или аналогичный Реестр ЕЭС, или в перечень российского ПО, разработанного и используемого для собственных нужд российскими юр.лицами**
3. ПО для ОБ ЗО КИИ и ГосСОПКА и/или обмена информацией о компьютерных инцидентах на объектах КИИ РФ, должно иметь сертификат соответствия ФСБ и/или ФСТЭК России
4. ПАК или ПАС, в случае реализации в нем функции защиты информации, сертифицирован ФСБ и/или ФСТЭК России

Вступление в силу предполагается с 01.09.2026 г.

Об импортозамещении и ПП №719

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

Постановлением Правительства РФ от 08.07.2025 года №1030 внесены изменения в ПП РФ 719
«О подтверждении производства российской промышленной продукции»

Установлены новые требования и балльная система, применяемые для оценки уровня локализации продукции с кодом ОКПД2:

- **26.20.40.140 «Средства защиты информации…» (для телеком. оборудования)**
- 26.30.11.110 «Средства связи, выполняющие функцию систем коммутации»
- 26.30.11.122 «Оборудование коммутации и маршрутизации пакетов информации сетей передачи данных»
- 26.30.23.141 «Оборудование систем передачи аудио-, видеоинформации для цифровой телефонии и конференцсвязи…»
- …

Изменена процедура включения изделий в Единый реестр российской радиоэлектронной продукции

Введены:

- дополнительная экспертная организация
- регламент взаимодействия с дополнительной экспертной организацией

Лицензирование деятельности
Об изменениях в ПП №171

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

Проект постановления Правительства РФ
«О внесении изменений в Положение о лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации, утвержденное постановлением Правительства Российской Федерации от 3 марта 2012 г. № 171»

Опубликован 10.04.2026

Проектом предусмотрены следующие изменения:

В дополнение к иностранными юр. лицам **НЕ ДОПУСКАЕТСЯ** осуществление лицензируемого вида деятельности:

- юр. лица, руководители которых имеют иностранное гражданство, ИП, имеющими иностранное гражданство

Увеличение минимального количества штатных инженерно-технических работников:

- **не менее 5 чел.** при разработке и/или производстве технических СЗИ;
- **не менее 10 чел.** при разработке и/или производстве программных (программно-технических) СЗИ.

Лицензиат будет обязан:

- использовать оборудование и программные средства преимущественно отечественного производства, расположенные на территории РФ
- иметь собственную аттестованную (или сертифицированную) ИС для обработки конфиденциальной информации непосредственно по месту осуществления деятельности

Для руководителей сокращается обязательный стаж работы в области лицензируемой деятельности, с 7 до 5 лет.

Дата вступления в силу 1 марта 2027 года

Лицензирование деятельности
Об изменениях в ПП №79

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

Проект постановления Правительства РФ

О внесении изменений в Положение о лицензировании деятельности по ТКЗИ, утвержденное постановлением Правительства РФ от 03.02.2012 г. № 79»

Опубликован 06.04.2026

Работы и услуги	Минимал. количество ИТР	Из них ИТР	Квалификационные требования		
			Образование	Стаж	Обязательная переподготовка по ИБ
Подпункты: «А», «Б», «Д», «Е» Контроль защищенности КИ от утечки по тех. каналам…, Контроль защищенности КИ от НСД и ее модификации в средствах и системах информатизации, Проектирование в защищенном исполнении: средств и систем информатизации …, Установка, монтаж, наладка, испытания, ремонт СЗИ	5	5	ВО по ИБ	от 3 лет	-
			Иное ВО		+
Подпункт: «Г» Проведение аттестационных испытаний и аттестации на соответствие требованиям по ЗИ: средств и систем информатизации и т.д.	9	3	ВО по ИБ	от 3 лет	-
			Ср. проф. по ИБ		
			Иное ВО		+
			Иное ср. проф.		
		6	ВО по ИБ	-	-
			Ср. проф. по ИБ		
			Иное ВО		+
			Иное ср. проф.		
Подпункт: «В» Мониторинг ИБ средств и систем информатизации	15	5	ВО по ИБ	от 3 лет	-
			Ср. проф. по ИБ		
			Иное ВО		+
			Иное ср. проф.		
		10	ВО по ИБ	-	-
			Ср. проф. по ИБ		
			Иное ВО		+
			Иное ср. проф.		
Независимо от вида выполняемых работ/оказываемых услуг	Руководитель	-	ВО по ИБ	от 3 лет	-
			Иное ВО	от 5 лет	+

Лицензионный контроль (ФСТЭК России)

Приказ ФСТЭК России от 12.05.2025 № 163
«Об установлении сроков и последовательности административных процедур при осуществлении ФСТЭК России и ее территориальными органами лицензионного контроля за деятельностью по ТЗКИ»

Приказ ФСТЭК России от 12.05.2025 № 164
«Об установлении сроков и последовательности административных процедур при осуществлении ФСТЭК России и ее территориальными органами лицензионного контроля за деятельностью по разработке и производству СЗКИ (в пределах компетенции ФСТЭК России)»

Приказом ФСТЭК России от 31.12.2025 № 487
Срок действия 163 и 164 приказов продлен до 31.12.2028

Ужесточение ответственности за нарушения в области защиты ПДн

Внесены изменения в УК РФ и КоАП РФ

(421-ФЗ и 420-ФЗ от 30.11.2024 от соответственно)

Вступили в силу с 30.05.2025

Правонарушение	Нарушитель	
	Должност.лицо	Организация
Незаконная передача информации 1-10 тыс. чел. или Утечка идентификаторов физ. лиц 10-100 тыс.	200-400 тыс. руб.	3-5 млн руб.
Незаконная передача информации 10-100 тыс. чел. или Утечка идентификаторов 100 тыс. – 1 млн чел.	300-500 тыс. руб.	5-10 млн руб.
Незаконная передача информации > 100 тыс. чел. или Утечка идентификаторов физ. лиц > 1 млн	400-600 тыс. руб.	10-15 млн руб.
Нелегальное распространение ПДн специальных категорий	1-1,3 млн руб.	10-15 млн руб.
Неправомерное распространение биометрических ПДн	1,3-1,5 млн руб.	15-20 млн руб.

С декабря 2024 года введена УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ за:

- неправомерное использование, передачу или хранение данных, полученных незаконным путем
- создание и обеспечение работы ресурсов, предназначенных для сбора и распространения таких данных
- нарушения, связанные с биометрией, данными несовершеннолетних и другими чувствительными категориями персональных данных

Компания выявила факт утечки:

1. Уведомить Роскомнадзор. **Срок – 24 часа**
2. Провести внутреннее расследование и подать итоговый отчет с указанием причин инцидента и лиц, ответственных за инцидент. **Срок – 72 часа**

Нарушение сроков – штраф до 3 млн рублей

Госконтроль. Обработка ПДн

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

Постановление Правительства РФ от 27.08.2025 № 1286
«О внесении изменений в постановление Правительства Российской Федерации от 29.06.2021 № 1046 «О федеральном государственном контроле (надзоре) за обработкой персональных данных»

Установлена следующая периодичность плановых контрольных (надзорных) мероприятий и обязательных профилактических визитов

Уровень риска объекта	Контрольные мероприятие	Профилактические визиты
Объекты высокого риска	1 контрольное мероприятие 1 раз в 2 года (или соответствующий профилакт. визит)	1 обязательный профилакт. визит в год (или соответствующее контрольн.мероприят)
Объекты значительного, среднего и умеренного риска	Не проводятся	Периодичность устанавливается Правительством РФ в соответствии с ФЗ «О гос. контроле…»
Объекты низкого риска	Не проводятся	Не проводятся

Профилактический, инспекционный визиты или выездные проверки могут проводиться с использованием ВКС или мобильного приложения «Инспектор»

Только российские (сертифицированные) средства защиты

Приказ ФСБ России от 18.03.2025 №117
«Об утверждении Требований о ЗИ, содержащейся в ГИС, иных ИС гос. органов, ГУП, гос. учреждений, с использованием шифровальных (криптографических) средств»

Указание Банка России от 18.02.2022 №6071-У
фактический **запрет на широкое использование ПЭП** для подтверждения транзакций в финансовых операциях с переходом на УНЭП, или УКЭП, или СКЗИ с функцией имитозащиты

Требования по обеспечению безопасности ЗО КИИ РФ, действующие с 1 января 2023 года
(в соответствии с Приказом ФСТЭК России от 20 февраля 2020 года №35)

- **СЗИ должны соответствовать** 6 или более высокому уровню доверия
- **Прикладное ПО,** планируемое к внедрению, **должно соответствовать**:
  - Требованиям по безопасной разработке ПО
  - Требованиям к испытаниям по выявлению уязвимостей в ПО
  - Требованиям к поддержке безопасности ПО

Приказы ФСТЭК России от 31 марта 2022 года № 61, от 15 апреля 2022 года № 66, от 15 апреля 2022 года № 67
об отзыве сертификатов СЗИ из недружественных иностранных государств и территорий, (всего отозвано 40 сертификатов)

50
сертифицированных продуктов ViPNet
(105 сертификатов)

60
сертификатов
получены в 2025 и начале 2026 года

Изменения в КоАП РФ. Последствия нарушения правил защиты информации

Федеральным законом от 23.05.2025 № 104-ФЗ внесены изменения в статью 13.12 КоАП РФ «Нарушение правил защиты информации»

Статья 13.12 КоАП РФ	Действующая редакция
Часть 2. Использование несертифицированных ИС, БД, а также несертифицированных СЗИ, если они подлежат обязательной сертификации (за исключением СЗИ, составляющей гос. тайну)	Граждане – от 5 до 10 тыс. руб. Долж. лица – от 10 до 50 тыс. руб. Юр. лица – от 50 до 100 тыс. руб.
Часть 4. Использование несертифицированных средств, предназначенных для защиты информации составляющей гос. тайну	Долж. лица – от 20 до 50 тыс. руб. Юр. лица – от 50 до 100 тыс. руб.
Часть 6. Нарушение требований о ЗИ (за исключением информации, составляющей гос. тайну), установленных ФЗ и принятых в соответствии с ними иными нормативными правовыми актами РФ	Граждане – от 5 до 10 тыс. руб. Долж. лица – от 10 до 50 тыс. руб. Юр. лица – от 50 до 100 тыс. руб.
Часть 7. Нарушение требований о защите информации, составляющей гос. тайну, установленных ФЗ и принятых в соответствии с ними иными нормативными правовыми актами РФ	Граждане – от 10 до 20 тыс. руб. Долж. лица – от 20 до 50 тыс. руб. Юр. лица – от 50 до 100 тыс. руб.

Увеличен установленный Статьей 4.5 срок давности привлечения к ответственности за административные нарушения, предусмотренные статьей 13.12, **ДО 1 ГОДА**

Ужесточение ответственности за утечки

Федеральный закон от 24.06.2025 № 175-ФЗ
«О внесении изменений в статью 183 УК РФ «Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну»

Вступил в силу с 05.07.2025

Введен нижний порог уголовного наказания за разглашение коммерческой, налоговой или банковской тайны

Разглашение	Наказание в виде лишения свободы	
	Минимум	Максимум
Совершено по корыстным мотивам, группой лиц или в случае крупного ущерба от преступления	2 года	5 лет
Влечет тяжкие последствия	3 года	7 лет

Дополнительно суды смогут штрафовать виновников утечек на суммы до 5 млн рублей

Порядок обращения с информацией «ДСП». Новые требования

Постановление Правительства РФ от 04.03.2026 года N 226

«О внесении изменений в постановление Правительства РФ от 03.11.1994 № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в ФОГВ, ГК «Росатом» и ГК «Роскосмос»

обязательно для

- федеральных органов гос. власти и гос. корпораций
- подведомственных им учреждений и организаций

рекомендовано для

- органов гос. власти субъектов
- иных гос. органов
- государственных внебюджетных фондов и организаций, которые осуществляют публично значимые функции

Регламентирует:

Порядок обращения с документами с пометкой «ДСП»

За что могут привлекать к ответственности:

- разглашение служебной информации
- нарушение порядка обращения с документами
- за использование служебной информации в личных и корыстных целях

САНКТ ПЕТЕРБУРГ

инфотекс

ТЕХНОФЕСТ

Академия инфотекс · Учебный центр инфотекс · AMPIRE · TELEOFIS · КОМФОРТЕЛ оператор связи бизнес-класса · РУТОКЕН компания ИНФОТЕКС · TS Solution · AXOFT

Подписывайтесь на наши соцсети