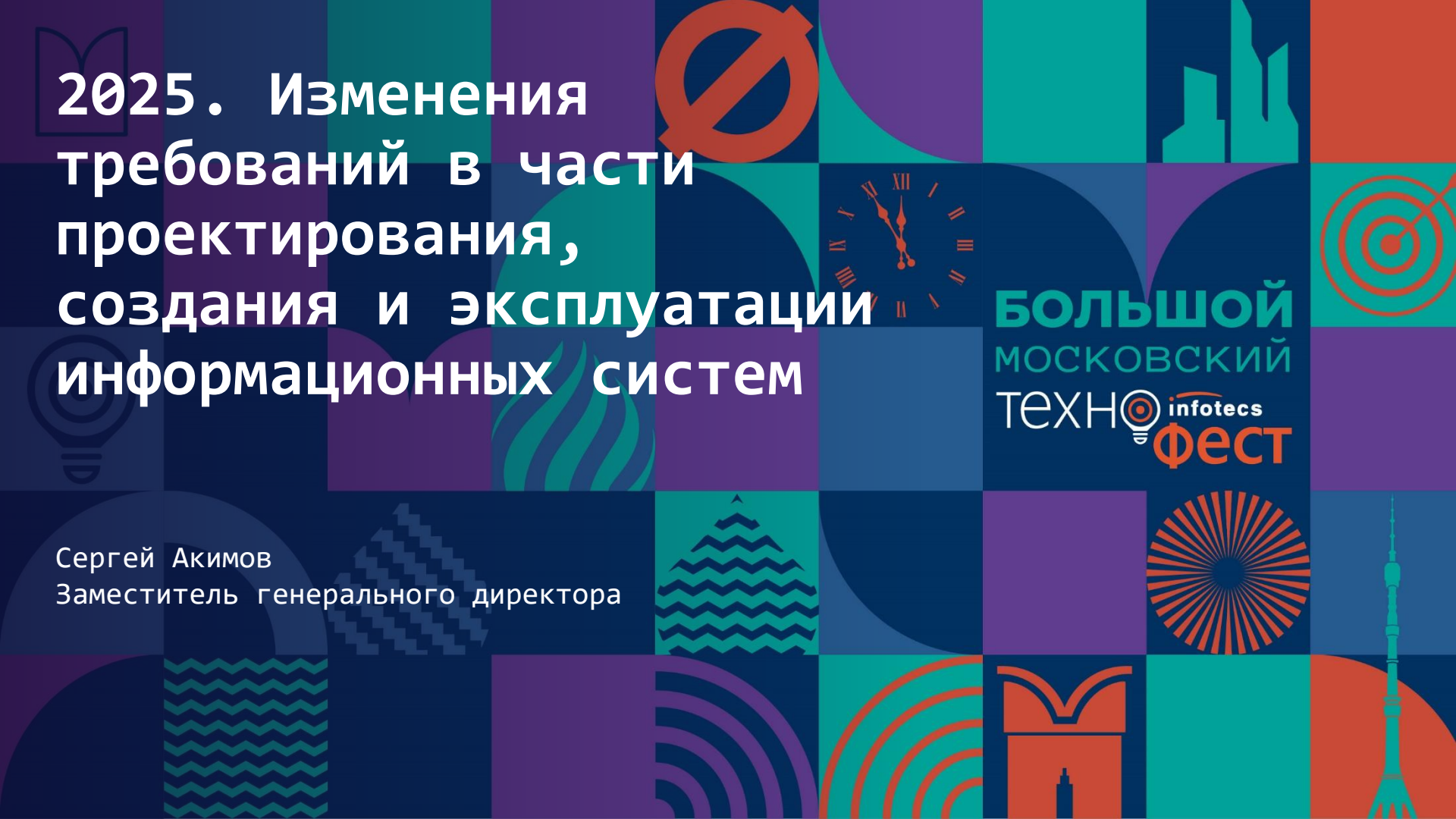
# 2025. Изменения требований в части проектирования, создания и эксплуатации информационных систем

Сергей Акимов
Заместитель генерального директора



# Тенденции 2022-2025 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»

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 **ЗАПРЕЩАЕТСЯ** использовать иностранное ПО на принадлежащих гос. органам ЗО КИИ, если иное не установлено ФЗ

с 1 января 2025 года **ЗАПРЕЩАЕТСЯ** 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 …

# Государственные информационные системы

## Приказ ФСТЭК России от 11.04.2025 №117

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

*Вступит 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**

## 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:

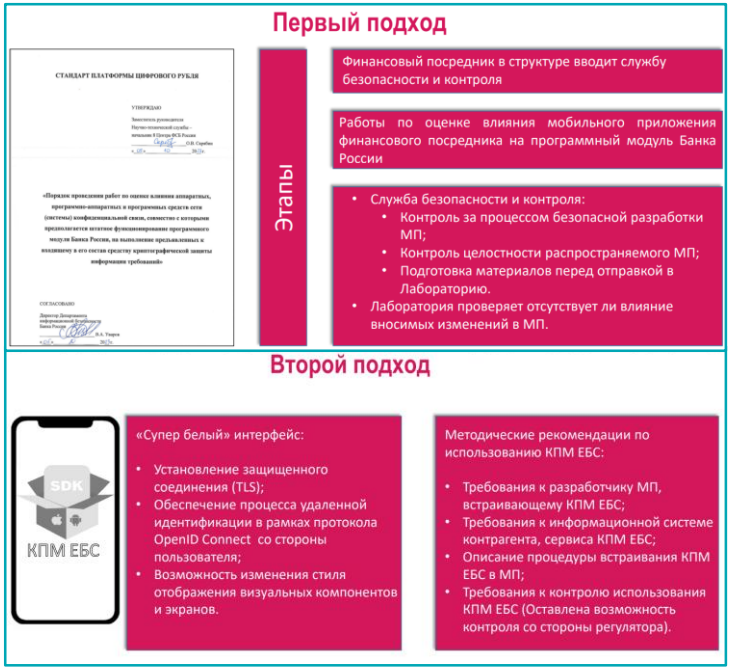
- Сферу действия (расширена относительно 524 приказа)
- Критерии обязательности применения СКЗИ в ИС
- Порядок определения требуемого класса СКЗИ

| 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 |

# О порядке проведения работ по оценке влияния на СКЗИ

Порядок проведения работ по оценке влияния аппаратных, программно-аппаратных и программных средств сети (системы) конфиденциальной связи, совместно с которыми предполагается штатное функционирование ПМБР, на выполнение, предъявляемых к входящему в его состав СКЗИ требований

(утвержден ФСБ России 05.10.2023)



# Изменения в ФЗ «О безопасности КИИ РФ»

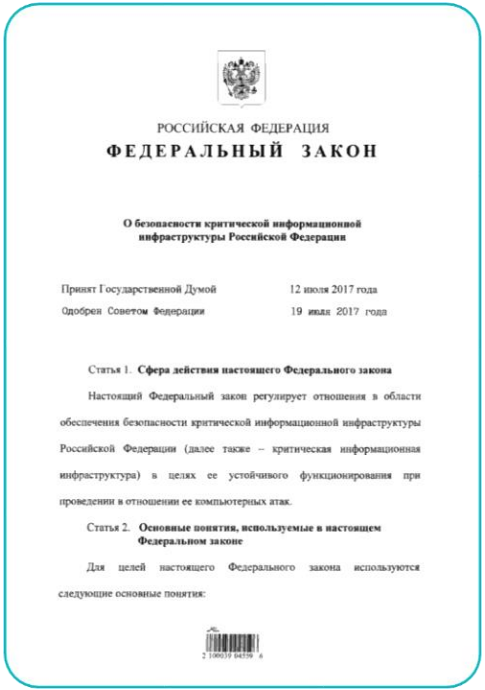
**Федеральный закон от 07.04.2025 N 58-ФЗ**
**«О внесении изменений в ФЗ «О безопасности КИИ РФ»**

*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
  *(подводятся итоги общественного обсуждения проекта постановления Правительства РФ №157304)*
- отраслевые особенности категорирования объектов КИИ
  *(обсуждаются проекты отраслевых особенностей категорирования объектов КИИ в 11 сферах)*
- требования к используемым на ЗО КИИ программно-аппаратным средствам
- порядок и сроки перехода субъектов КИИ на использование российского ПО
  *(19.09.2025 опубликован проект постановления Правительства РФ №159943)*
- порядок осуществления мониторинга за исполнением субъектами КИИ обязанности по использованию на ЗО КИИ ПО, указанного в п.5 ч.3 статьи 9 187-ФЗ
  *(19.09.2025 опубликован проект постановления Правительства РФ №159847)*
- …



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:

# Исполнение ФЗ «О безопасности КИИ РФ»

ТЕХНО infotecs ФЕСТ

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

**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…»**

*Опубликован 19.09.2025*

**Проектом устанавливаются:**

- Сроки перехода – до 01.01.2028
  (в отдельных случаях до 01.12.2030)
- Правила перехода
- Ответственные за организацию перехода ФОИВ и организации
- **Дата вступления в силу – 01.04.2026**

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

**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»**

*Опубликован 19.09.2025*

**Проектом устанавливаются:**

- Порядок осуществления мониторинга
- ФОИВ и организации, осуществляющие мониторинг
- **Дата вступления в силу – 01.04.2026**

# Изменения в категорировании ЗО КИИ

**Проект постановления Правительства Российской Федерации**

**«Об утверждении Перечней типовых отраслевых объектов критической информационной инфраструктуры»**

*Опубликован 04.06.2025*

Для каждой из 8 сфер КИИ в проекте представлены типовые объекты (ИС, ИТКС, АСУ), типовые процессы или функции, выполняемые объектом, и виды деятельности, для обеспечения которых используется типовой объект

**Проект постановления Правительства Российской Федерации**

**«О внесении изменений в ПП РФ от 8 февраля 2018 года № 127 «Об утверждении Правил категорирования объектов КИИ РФ, а также перечня показателей критериев значимости объектов КИИ РФ и их значений»**

*Опубликован 10.06.2025*

**Согласно изменениям:**

- установление соответствия объекта КИИ критериям значимости, расчет значений показателей критериев значимости и присвоение объекту КИИ одной из категорий значимости должны будут 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»

*Оба проекта находятся на стадии подведения итогов общественного обсуждения*

# Оценка обеспечения безопасности объектов КИИ*

По результатам государственного контроля выявлено более **800** нарушений

В более **40%** имелась реальная угроза нарушения устойчивого функционирования ЗО КИИ

Составлено протоколов об административных правонарушениях:

*статья 13.12.1* ***31*** *дело*

*статья 19.7.15* ***123*** *дела*

***Типовые нарушения:***

- несоответствие фактического состава значимых объектов КИИ сведениям, включенным в реестр значимых объектов КИИ
- Некатегорирование объектов КИИ, соответствующих типовому перечню
- отсутствие контроля за действиями организаций-подрядчиков, которым разрешен доступ к ПО и ПАК значимых объектов КИИ
- непроведение мероприятий по выявлению и анализу уязвимостей на значимых объектах КИИ, наличие уязвимого ПО на значимых объектах КИИ
- отсутствие компенсирующих мер, обеспечивающих блокирование угроз безопасности информации
- отсутствие обновления антивирусных баз
- администрирование осуществляется с рабочих мест, находящихся в корпоративных сетях, имеющих выход в Интернет, без реализованных мер обеспечения безопасности

7

* - по материалам выступления Елены Борисовны Торбенко

# 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.б)*

## 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 ЗОКИИ **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** | 47 записей |
| 2 | ПО, используемое в составе ПАК ViPNet в **Реестре Минцифры России** | 59 записей |
| 3 | Наличие действующих сертификатов соответствия **ФСБ России** для ПАК ViPNet | 58 сертификатов |
| | Наличие действующих сертификатов соответствия **ФСТЭК России** для ПАК ViPNet | 5 сертификатов |

Порядка 50 ПАК ViPNet сегодня полностью удовлетворяют требованиям и могут быть признаны доверенными

# Импортозамещение. Изменения в ПП №719 и №878

ТЕХНО infotecs ФЕСТ

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

**Постановлением Правительства РФ от 8 июля 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…»
- …

**Постановлением внесены изменения в процедуру включения изделий в Единый реестр российской радиоэлектронной продукции**

**Вводятся:**

- дополнительная экспертная организация
- регламент взаимодействия с дополнительной экспертной организацией

# Лицензирование деятельности (ФСТЭК России)

**Приказ ФСТЭК России от 10.12.2024 N 227**
«Об утверждении Программы профилактики нарушении лицензионных требований, соблюдение которых оценивается при проведении ФСТЭК России лицензионного контроля за деятельностью по ТЗКИ и деятельностью по разработке и производству СЗКИ, на 2025 год»

**Информационное сообщение ФСТЭК России от 26.12.2024 № 240/13/6597**
«О разработанных ФСТЭК России в новой редакции перечней НПА, метод. док. и нац. стандартов, необходимых для выполнения работ и (или) услуг по лицензированию деятельности по ТЗКИ и деятельности по разработке и производству СЗКИ»

**Лицензиаты ФСТЭК России должны соответствовать новыми перечням – с 1 сентября 2025 года**

**Приказ ФСТЭК России от 19 декабря 2024 N 237**
«Об утверждении программы профилактики нарушений обязательных требований, соблюдение которых оценивается при проведении ФСТЭК России мероприятий по контролю в рамках гос. контроля за соблюдением российскими участниками внешнеэконом. деятельности законодательства РФ в области экспортного контроля, на 2025 год»

**Информационное сообщение ФСТЭК России от 28 марта 2025 N 240/13/1729**
«О перечне НПА, содержащих обязательные требования, соблюдение которых оценивается при лицензировании деятельности по ТЗКИ и деятельности по разработке и производству СЗКИ»

# 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)»**

# Лицензирование деятельности (ФСБ России)

**Приказ ФСБ России от 16.11.2024 №479**
**«О внесении изменений в приказ ФСБ России от 31.01.2022 №35 «Об утверждении форм документов, используемых ФСБ России в процессе лицензирования в соответствии ФЗ «О лицензировании отдельных видов деятельности»**

Внесены корректировки в некоторые документы, используемые при лицензировании, а также введены несколько дополнительных форм:

- заявление юр.лица / ИП о предоставлении лицензии
- заявление юр.лица / ИП о внесении изменений в соответствующий реестр
- заявление юр.лица / ИП о прекращении лицензируемого вида деятельности
- заявление о предоставлении сведений о лицензии

# 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

ТЕХНО infotecs ФЕСТ

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»**

Устанавливается 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 недружественных иностранных государств и территорий, (всего отозвано 40 сертификатов)

**43**
**сертифицированных продукта ViPNet**
(104 сертификата)

**68**
**сертификатов**
получены в 2024 и 2025 годах

# 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.<br>**Долж. лица** – от 10 до 50 тыс. руб.<br>**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.<br>**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.<br>**Долж. лица** – от 10 до 50 тыс. руб.<br>**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.<br>**Долж. лица** – от 20 до 50 тыс. руб.<br>**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

ТЕХНО infotecs ФЕСТ

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

**Проект Постановления Правительства РФ**

**«О внесении изменений в постановление Правительства РФ от 03.11.1994 № 1233»**

*Завершение независимой антикоррупционной экспертизы*

**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:**

**Как обращаться с документами ДСП**

создавать, передавать, хранить, уничтожать документы ДСП

**За что сотрудника могут привлекать:**

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

# Эксперимент по повышению уровня защищенности ГИС ФОИВ и подведомственных им учреждений

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

**Постановление Правительства РФ от 26.03.2025 № 372**
**«Эксперимент по повышению уровня защищенности ГИС ФОИВ и подведомственных им учреждений»**

**Предусматривает проведение эксперимента с 01.04.2025 по 31.12.2027**

**Участники эксперимента:**

- Минцифры России
- ФСБ России
- ФСТЭК России
- Гос. учреждения, подведомственные ФОИВ (по согласованию с ФОИВ)
- Иные учреждения, привлекаемые Минцифры России, указанные в утвержденном Положении

**Цели эксперимента:**

- независимая оценка текущего уровня защищенности ГИС
- сбор информации о системах ЗИ, размещенной в ГИС, выявление недостатков (уязвимости) СЗИ и ПО, применяемых в ГИС, оценка возможности их использования нарушителем
- проверка практической возможности использования нарушителем выявленных недостатков (уязвимости) СЗИ и ПО, применяемых в ГИС
- разработка перечня мер, нейтрализующих выявленные в ГИС уязвимости
- проведение мероприятий по устранению выявленных в ГИС недостатков (уязвимостей)

# ГИС по противодействию правонарушениям

**Федеральный закон от 01.04.2025 N 41-ФЗ**
**«О создании ГИС противодействия правонарушениям, совершаемым с использованием ИКТ, и о внесении изменений в отдельные законодательные акты РФ»**

*Вступил в силу с 01.06.2025*

Минцифры создаст ГИС для сбора от организаций и граждан данных о киберпреступлениях. Эти данные по запросу на условиях конфиденциальности смогут получать МВД и СК РФ

**В соответствии с ФЗ:**
**Сотрудникам организаций госсектора и финансовых учреждений будет запрещено вести служебное общение с гражданами в иностранных мессенджерах**

# Внимание, прецедент!

РОСКОМНАДЗОР

## Банк оштрафован на 200 тыс. рублей за пересылку персональных данных в WhatsApp

Версия для печати

15 АПРЕЛЯ 2025 ГОДА

Российский суд впервые привлек к ответственности финансовую организацию за использование иностранного мессенджера для передачи персональных данных гражданина.

С доказательствами нарушения банком закона в Роскомнадзор обратилась жительница Москвы. В ходе разбирательства выяснилось, что сотрудник кредитной организации, вопреки запрету, отправил с корпоративного номера сообщение должнику через WhatsApp.

Банк был признан виновным по статье 13.11.2 КоАП и оштрафован на 200 тыс. рублей за коммуникацию с должником через WhatsApp.

С 1 марта 2023 года в силу вступил запрет на использования иностранных мессенджеров при оказании финансовых и государственных услуг. Роскомнадзор перечислил мессенджеры, запрещенные для передачи платежных документов и ПД россиян.

В конце июня 2023 года Госдума ввела штрафы до 700 тыс. рублей для финансовых организаций и госструктур за пересылку юридически значимых документов в иностранных мессенджерах. Закон был принят для защиты персональных данных россиян.

Время публикации: 15.04.2025 16:51
Последнее изменение: 15.04.2025 16:52

# ТЕХНО infotecs ФЕСТ

Подписывайтесь
на наши соцсети,
там много интересного

CYBER MEDIA
NBJ НАЦИОНАЛЬНЫЙ БАНКОВСКИЙ ЖУРНАЛ
GLOBAL DIGITAL SPACE
CISOCLUB
РУТОКЕН
ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ
АВАНГАРД
AR integ
АТБ ЭЛЕКТРОНИКА
infotecs {/-cademy}
merlion
УЧЕБНЫЙ ЦЕНТР ИНФОТЕКС