Обеспечение безопасности информации согласно 117 приказу ФСТЭК России

Сегодня обсудим

- Что изменилось по сравнению с 17-ым приказом
- На кого распространяется новый приказ
- Как меняется подход к защите информации
- Позиция регулятора
- Ключевые действия в 2025 и 2026 году

Приказ ФСТЭК России № 117 от 11.04.2025 (опубликован 16.06.2025)

Вступает в силу с 01 марта 2026 года и полностью заменит приказ ФСТЭК № 17

Расширяется перечень организаций, на которые распространяется действие приказа (по сравнению с приказом №17)

Расширяется область применения внутри организации

Трансформируется подход по защите информации от «бумажной» к эффективной

	Приказ ФСТЭК № 17	Приказ ФСТЭК № 117
Что	Только государственные (и в отдельных случаях муниципальные) информационные системы	Все ИС государственных органов, государственных унитарных предприятий, государственных учреждений
Кто	Только операторы ГИС (и в отдельных случаях МИС)	Практически все ГО, ГУП, ГУ Подрядные организации
Группы мер защиты	13	17
Формы оценки	Аттестация	Аттестация Показатель защищённости Показатель уровня зрелости

Область действия

Государственные органы

- Правительства (кроме Аппарата Правительства РФ)
- Суды (кроме Конституционного и Верхного)
- Прокуратура РФ
- Государственные комитеты РФ
- Региональные министерства и департаменты

Государственные унитарные предприятия

- Водоканалы, Теплосети, Электросети
- Сфера ЖКХ
- Транспорт
- Фармацевтика (аптеки, производство)
- Промышленность
- НИИ
- СМИ (в т.ч. производство материалов для СМИ, киностудии)

Государственные учреждения

- Лечебные организации
- Образовательные учреждения
- Театры, музеи, библиотеки
- Социальные центры
- МФЦ
- ФОМС и ТФОМС
- Спортивные учреждения

Новый подход

Учёт современных технологий: ИИ, контейнеризация, облачные технологии, IoT

Переход на процессный подход к защите информации

Контроль цепочки поставок

Требования к персоналу и документации

Процессный подход

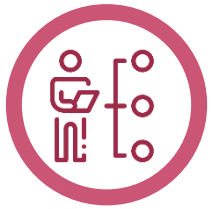
Оценка эффективности

Аттестация

только для ГИС, бессрочно (до внесения критичных изменений)

Показатель защищенности (КЗИ)

для всех ИС, раз в 6 месяцев

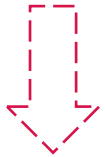


Показатель зрелости (ПЗИ)

для всех ИС, раз в 2 года

Регламентации деятельности по защите информации

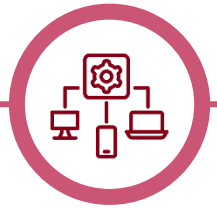
Политика защиты информации



Стандарты по защите информации, устанавливающие требования к реализации мер по защите информации

Регламенты по защите информации, содержащие порядок проведения мероприятий или описание реализуемых процессов по защите информации

Технические меры защиты



Защита конечных устройств и пользователей

- идентификация и аутентификация
- управление доступом
- защита конечных устройств
- антивирусная защита
- регистрация событий безопасности

Сетевая безопасность

- защита точек беспроводного доступа
- обнаружение и предотвращение вторжений на сетевом уровне
- сегментация и межсетевое экранирование
- защита от компьютерных атак, направленных на отказ в обслуживании
- защита каналов передачи данных и сетевого взаимодействия

Новые технические меры защиты

- виртуализации и облачных вычислений
- сервисов электронной почты
- веб-технологий
- программных интерфейсов взаимодействия приложений
- мобильных устройств
- технологий интернета вещей

Работа с подрядчиками

Для кого

- Организации, получающие информацию из государственных информационных систем
- Сторонние организации, привлекаемые для разработки программного обеспечения
- Организации, обеспечивающие поддержку информационных систем или защиту информации в них

Что необходимо сделать

- Разработать регламент предоставления доступа к ИС
- Включить требования по безопасной разработке ПО (если ведётся внешняя разработка)
- Контролировать выполнение мер по ИБ в ИС подрядных организациях

Требования к безопасной разработке ПО

- ГОСТ Р 56939-2024 включает в себя 24 процесса, которые покрывают почти весь жизненный цикл разработки ПО
- Приказ №117 дополняет требования ГОСТа в части защиты технологий контейнерных сред и их оркестрации, использование WAF
- ГОСТ Р 56939-2024 содержит в том числе методику оценки соответствия требованиям ГОСТ

Приказ ФСТЭК России № 117

- СЗИ без криптографии
- Требования к документации
- Требования к классам СЗИ

Приказ ФСБ России № 117

- СКЗИ
- Требования к помещению, где есть СКЗИ
- Требования к классам СКЗИ

Алгоритм действий

Государственные информационные системы организации (ГИС)	○ Пересмотреть существующую систему защиты информации с учетом новых требований по защите ○ Пересмотреть комплект ОРД, регламентировать новые процессы ○ Сохраняется требование по аттестации
Иные информационные системы организации	○ Определить перечень иных информационных систем и перечень мер защиты, которые требуется реализовать в отношении этих систем ○ Учесть иные информационные системы в комплекте организационно-распорядительной документации ○ Провести оценку соответствия
Информационные системы контрагентов, взаимодействующие с ИС	○ Определить порядок взаимодействия с информационными системами подрядчиков ○ Разработать требования для подрядчиков ○ Определить порядок подтверждения выполнения требований со стороны подрядчиков

Ключевые действия

в 2025 году:

1. Провести обследование информационных систем
2. Сформировать перечень негативных последствий
3. Оценить состояние защиты информации
4. Провести ревизию подрядчиков
5. Разработать план мероприятий по совершенствованию защиты информации и дорожную карту

в 2026 году:

1. Разработать политику, стандарты и регламенты
2. Закупить, внедрить и настроить дополнительные СрЗИ
3. Внедрить процессы управления ИБ, в т.ч. процесс обеспечения непрерывности и процесс безопасной разработки ПО
4. Организовать повышение уровня знаний пользователей ИС
5. Подтвердить достаточность принятых мер защиты ИС в форме аттестации или контроля уровня защищенности информации

Чем мы можем помочь

- Проведение аудита и выявление информационных систем
- Определение негативных событий
- Оценка угроз безопасности и необходимых мер защиты информации

- Разработка необходимой документации: политика защиты информации, стандарты и регламенты, требования по информационной безопасности для подрядных организаций
- Проектирование системы защиты информации
- Поставка, внедрение и сопровождение необходимых средств защиты информации
- Обеспечение непрерывности деятельности

- Оценка защищённости информационных систем
- Оценка зрелости процессов обеспечения защиты информации
- Аттестация государственных информационных систем
- Внедрение процессов безопасной разработки программного обеспечения в соответствии с ГОСТ Р 56939-2024

Остались вопросы?
На них ответит Юлия Смолина,
руководитель центра компетенций по
консалтингу ИБ
y.smolina@softline.com