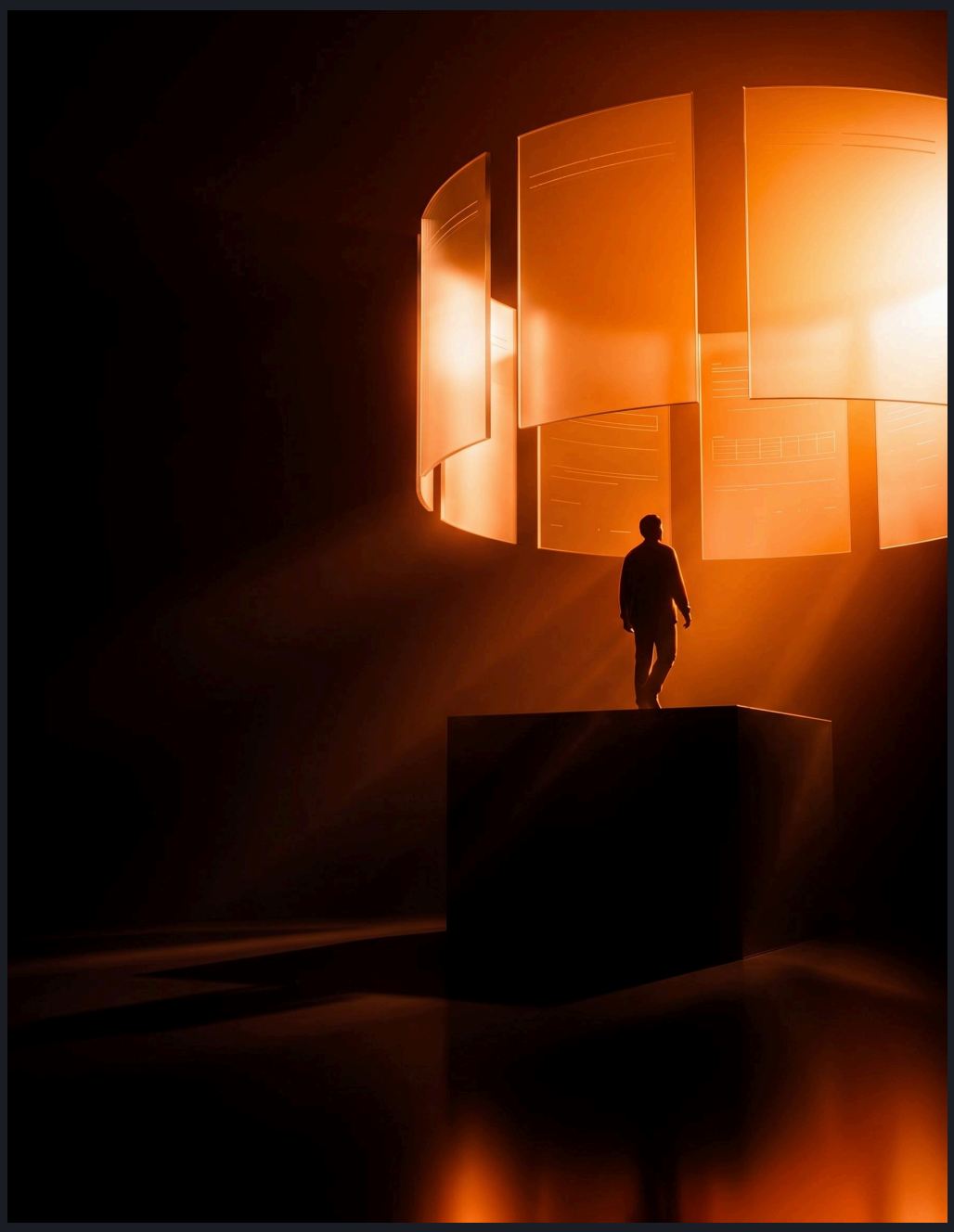
SOLAR

Практическое руководство по проверке защиты информации (ИОД) на соответствие требованиям приказа ФСТЭК России № 117

На примере DLP-системы Solar Dozor



Для специалистов
и руководителей ИБ государственных органов, ГУП, госучреждений

Не является официальным разъяснением регулятора. Подготовлено на основе приказа ФСТЭК России № 117 от 11.04.2025 и методического документа от 12.04.2026.

W: RT-SOLAR.RU

T: 8 (800) 302-85-23

Что изменил приказ № 117

Приказ № 17 утратил силу

Организации, работавшие по его требованиям, обязаны привести системы защиты в соответствие с приказом № 117. Информационные системы, аттестованные по приказу № 17, переаттестации не подлежат — но только до первой модернизации. При последующей аттестации применяются требования приказа № 117. При наличии актуальной угрозы утечки ИОД отсутствие DLP-системы будет зафиксировано как несоответствие пп. 30а и 40.

Новый приказ охватывает все информационные системы государственных органов, ГУП и госучреждений — не только аттестуемые ГИС. Особое внимание уделяется защите информации ограниченного доступа (ИОД) — это персональные данные, служебная тайна, сведения с пометкой «для служебного пользования» и любая другая информация, доступ к которой ограничен законодательством.

01.03.2026

Дата вступления в силу

≥30%

Сотрудников ИБ с профильным образованием

6 мес.

Периодичность оценки защищенности КЗИ

2 года

Периодичность оценки зрелости ПЗИ

ИЗМЕНЕНИЕ	СУТЬ
Расширен периметр защиты	Требования распространяются на все ИС органов, а не только на ГИС. Обязательная аттестация — только для ГИС
DLP назван явно среди обязательных классов СЗИ	Приказ впервые прямо указывает на необходимость применения конкретных классов СЗИ: DLP, SWG, NGFW, NTA, PAM
Новые требования к защите ИОД при обработке	Пп. 30а, 40: необходимо исключить утечку и неправомерное распространение ИОД в любой форме, включая интернет
Обязательные мероприятия по подготовке персонала	Не менее 30% состава подразделения ЗИ должны иметь профильное образование или переподготовку
Методический документ ФСТЭК от 12.04.2026	Детализирует состав и содержание мероприятий — теперь есть конкретный перечень того, что должна уметь СЗИ

Почему средств от НСД недостаточно

По данным расследований инцидентов, большинство утечек ИОД реализуется не внешними нарушителями, а пользователями с легитимным доступом к информации. Средства разграничения доступа такие нарушения не выявляют: пользователь авторизован, канал передачи разрешен. Приказ № 117 прямо указывает на необходимость применения DLP как отдельного класса СЗИ.

УГРОЗА	ПОЧЕМУ СЗИ ОТ НСД НЕ ПОМОГАЕТ	СЗИ ОТ НСД	DLP
Умышленная утечка сотрудника/подрядчика	Действует от имени легальной учетной записи, использует разрешенные каналы	Нет	Да
Неумышленная утечка по невнимательности	Ошибку совершает пользователь с легально предоставленными правами доступа	Нет	Да
Неправильное хранение ИОД на файловых ресурсах	Документ размещен на ресурсе, доступном посторонним	Нет	Да
Утечка с мобильных и удаленных рабочих мест	Обработка ведется вне офиса, вне периметра контроля средств от НСД	Нет	Да
Скрытая подготовка к утечке (инсайдер)	На ранней стадии нет факта передачи — только аномальное поведение в рамках предоставленных прав	Нет	Да

Требование приказа № 117, п. 40:

Мероприятия по защите информации при обработке, хранении и обращении с ИОД должны исключать неправомерное распространение ИОД вне зависимости от формы ее представления, в том числе с использованием информационно-телекоммуникационных сетей и сети Интернет.

Нормативный маппинг

Конкретные пункты приказа № 117 и методического документа от 12.04.2026 с прямым указанием, как именно DLP обеспечивает их выполнение.

ПУНКТ	СУТЬ ТРЕБОВАНИЯ	КАК SOLAR DOZOR ЗАКРЫВАЕТ
п. 30а	Исключение утечки ИОД и иной конфиденциальной информации	Перехват и анализ трафика на всех каналах передачи. При обнаружении — блокировка или оповещение офицера ИБ в реальном времени
п. 40	Исключение неправомерного распространения ИОД вне зависимости от формы, включая Интернет	Контроль почты, веба, мессенджеров, файлов, печати, USB. Морфологический анализ содержимого — находит ИОД в любом формате, в том числе в архивах и изображениях
пп. 42, 45	Защита при использовании мобильных устройств	Агенты для Windows, Linux, macOS контролируют действия на рабочем месте независимо от сети
п. 46	Защита при удаленном доступе	Агентский контроль всех коммуникаций при удаленной работе; интеграция с точками сетевого перехвата
п. 47	Защита при беспроводном доступе	Контроль каналов передачи данных через агентские и сетевые компоненты при подключении через Wi-Fi и мобильные сети, включая «белые» и «черные» списки сетей Wi-Fi
пп. 14, 20–21, 26	Организация деятельности по ЗИ: стандарты, регламенты, роли	Единая консоль с ролевым доступом, журналы действий, отчеты для подготовки регламентов обращения с ИОД и контроля их исполнения
Метод. док	СЗИ должна быть источником событий для SIEM и обеспечивать сохранность архива	MultiConnector передает события в SIEM/SOAR. Кластерная архитектура с оперативным и долгосрочным архивами
п. 63е	Защита сервисов электронной почты. Новая группа из шести мер	Mail Connector и модуль фильтрации сообщений перехватывают и анализируют трафик. Контентный анализ блокирует передачу ИОД
пп. 40, 30а	Защита информации при обработке, хранении и обращении с ИОД	DLP + SWG + PAM — контроль передачи. NGFW с DPI + DLP + SWG — мера ЗКС.4. File Crawler — выявление нарушений хранения
Метод. п. 3.16	Защита информации при взаимодействии с подрядчиками	Solar Dozor контролирует действия подрядчиков через агентские компоненты. UBA выявляет аномалии. Граф связей фиксирует коммуникации

Функциональные возможности Solar Dozor в контексте приказа № 117

Приказ № 117 рассматривает защиту информации как непрерывный циклический процесс. Solar Dozor обеспечивает реализацию четырех ключевых функций в рамках этого процесса.

НАИМЕНОВАНИЕ	ПРАКТИЧЕСКАЯ ЦЕННОСТЬ	ФУНКЦИОНАЛ
Исключение утечки ИОД и иной конфиденциальной информации	Все действия с ИОД отображаются в едином интерфейсе; данные передаются в корпоративный SIEM без ручного сбора из разных источников	События и инциденты · Журналы и отчеты · MultiConnector · Интеграция с SIEM/ SOAR/XDR
Инструмент реагирования	Передача ИОД блокируется в момент нарушения. Ответственный специалист получает оповещение до того, как информация покинула периметр	Блокировка в реальном времени · Оповещение · Карантин · Активный режим File Crawler
Инструмент расследования	При инциденте или запросе аттестатора — полная история коммуникаций, граф связей, доказательная база. Подготовка материалов для Роскомнадзора в установленные сроки	Досье персоны · Модуль расследований · Долговременный архив · Граф связей
Инструмент профилактики	Выявляет признаки инсайдерской активности до факта утечки: аномальное поведение, копирование данных, подготовку к уходу	UBA — анализ поведения · Профили пользователей · Группы риска · Выявление аномалий

Комплексное закрытие требований:

DLP + SWG + PAM — контроль передачи и распространения ИОД в ИС и за ее пределами (пп. 30а, 40, 46, 47). NGFW с DPI + DLP + SWG — реализация меры ЗКС.4. File Crawler — инспекция файловых ресурсов и обнаружение нарушений правил хранения ИОД (п. 40).

Solar Dozor в госсекторе: реальные внедрения

Solar Dozor применяется в федеральных органах исполнительной власти, территориально распределенных организациях и муниципальных структурах. Ниже приведены примеры внедрения.

МКУ «ЦЕНТР ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ГОРОДСКОГО ОКРУГА „ГОРОД ЯКУТСК“»

Масштаб

200+ рабочих станций

Контур

Городская инфраструктура и все подразделения администрации

Задача

Мониторинг событий безопасности и реагирование на них в распределенной муниципальной структуре

Результат

Подтверждена применимость Solar Dozor для муниципального контура и задач регистрации событий ИБ

ФЕДЕРАЛЬНЫЙ ОРГАН ИСПОЛНИТЕЛЬНОЙ ВЛАСТИ

Масштаб

2500+ рабочих станций

Контур

Совместное внедрение Solar Dozor и Solar addVisor

Задача

Защита данных в крупной распределенной инфраструктуре ФОИВ с поведенческой аналитикой персонала

Результат

Подтверждены масштабируемость и поддержка сложной инфраструктуры; сочетание DLP с аналитикой поведения

ПРЕДПРИЯТИЕ ГОСУДАРСТВЕННОГО СЕКТОРА

Масштаб

2000+ рабочих станций

Контур

Совместно с Solar webProxy; головной офис и два территориальных подразделения

Задача

Единая политика безопасности для территориально распределенной структуры с общим досье по сотрудникам

Результат

Подтверждена пригодность решения для распределенной госструктуры с централизованным управлением

Базовый план перехода на требования приказа № 117

ФСТЭК настоятельно рекомендует разработать план перехода со сроками. Наличие такого плана на момент аттестации снижает риск замечаний — регулятор видит, что организация осознала изменения и движется к соответствию.

01

Оценить актуальность угрозы утечки

Проверить БДУ ФСТЭК: если угроза утечки ИОД актуальна, DLP становится обязательным.

02

Обновить политику ЗИ и МУиН

Включить угрозы конфиденциальности в МУиН. Разработать или актуализировать регламенты обращения с ИОД.

03

Определить каналы и объекты защиты

Составить перечень каналов: почта, веб, мессенджеры, съемные носители, удаленный доступ.

04

Определить требования к подрядчикам

Предъявить требования по ЗИ подрядчикам, создать для них отдельные учетные записи.

05

Внедрить DLP

Настроить политики Solar Dozor. Запустить пилот, расширить охват, подключить File Crawler.

06

Интегрировать с SIEM и выстроить процессы

Подключить Solar Dozor как источник событий. Назначить роли, прописать регламенты реагирования.

07

Зафиксировать в «Плане совершенствования ЗИ»

Наличие плана фиксирует готовность организации и учитывается при аттестации.

Оценка текущего уровня готовности

Отметьте выполненные пункты. Незакрытые позиции указывают на несоответствия, которые подлежат устранению до проведения аттестационных испытаний.

Комплексное закрытие требований

- [ ] Политика защиты информации организации разработана и утверждена
- [ ] Стандарты и регламенты по ЗИ актуализированы под требования приказа № 117
- [ ] Модель угроз и нарушителей обновлена с учетом угроз утечки ИОД
- [ ] План перехода на требования приказа № 117 составлен и утвержден
- [ ] ≥30% состава подразделения ЗИ имеют профильное образование
- [ ] Уровни значимости определены для всех ИС (ИОД с пометкой «ДСП» — УЗ 1)

Технические меры (DLP)

- [ ] Все каналы передачи и хранения ИОД определены и задокументированы
- [ ] DLP-система охватывает каналы: почта, веб, мессенджеры, файлы, печать, USB-носители
- [ ] Агенты DLP установлены на всех рабочих станциях, включая удаленные и мобильные
- [ ] File Crawler проведен — нарушения правил хранения ИОД устранены
- [ ] DLP интегрирована с SIEM как источник событий безопасности
- [ ] UBA настроен — анализ поведения пользователей запущен
- [ ] Политики блокировки и регламент реагирования офицера ИБ определены
- [ ] Защита электронной почты настроена: Mail Connector, антиспам, контентный анализ
- [ ] Для подрядчиков созданы отдельные учетные записи, их действия контролируются

Контроль и аттестация

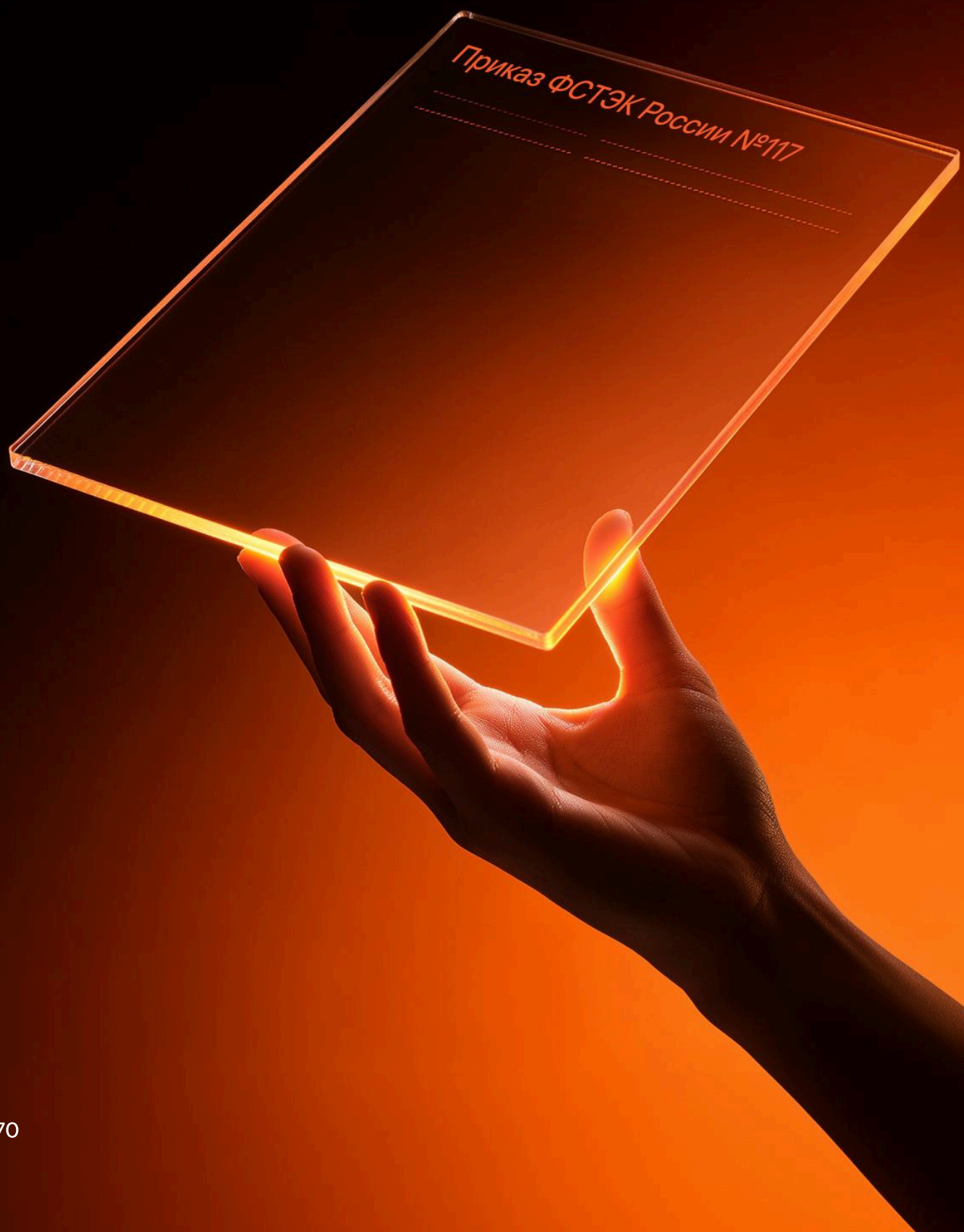
- [ ] Оценка показателя защищенности КЗИ проводится не реже 1 раза в 6 месяцев
- [ ] Оценка показателя уровня зрелости ПЗИ запланирована (не реже 1 раза в 2 года)
- [ ] Периодический контроль уровня защищенности запланирован (не реже 1 раза в 3 года)
- [ ] Аттестация ИС проведена или запланирована в соответствии с приказом № 117

Остались вопросы?

Получите консультацию специалиста
по применению DLP-системы Solar Dozor
на соответствие требованиям приказа
№ 117 ФСТЭК

Не является официальным разъяснением регулятора.
Подготовлено на основе приказа ФСТЭК России № 117
от 11.04.2025 и методического документа от 12.04.2026.

Запросить консультацию



T: +7 (499) 755-07-70

E: info@rt-solar.ru