

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ · 2026

После приказа № 21: как меняется модель защиты персональных данных

Что меняется, что письменно разъяснил регулятор и как подготовиться к переходу

Шихвердиева Алина Шихвелиевна

Главный инженер-проектировщик систем информационной безопасности

План доклада

01

Контекст и проблема

Почему приказ № 21 устарел и что сейчас с проектом



02

Анализ реформы

Риск-ориентированная модель, новые направления, Узи



03

Разъяснения ФСТЭК России

Два письменных ответа на официальные запросы



04

План подготовки

Аудит → разрыв-анализ → приоритизация → документы

Три главные мысли



Перечень → риски



Новые направления + Узи



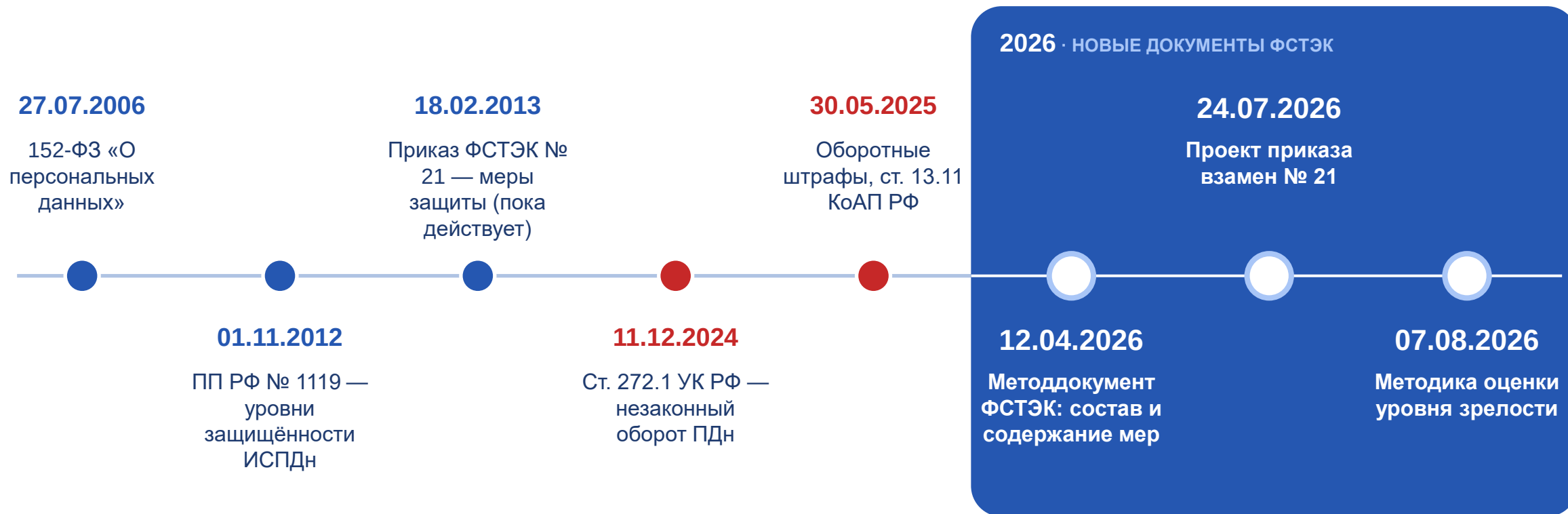
Разъяснения регулятора

01

Контекст и постановка проблемы

Почему модель 2013 года больше не работает

Ключевые НПА по защите ПДн: на что смотреть в 2026 году



Дата вступления нового приказа — не определена. В проекте указано 01.09.2026, но на эту дату приказ не был принят. ФСТЭК России письменно сообщил, что дата будет скорректирована. Сейчас действует приказ № 21.

Модель приказа № 21 не успевает за технологиями

13

лет приказ № 21 определяет защиту
ПДн: оператор выбирает меры из
фиксированного перечня по уровню
защищённости

Чего в модели 2013 года нет как категорий



Облака



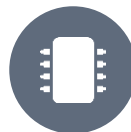
Контейнеры и
оркестрация



API-интеграции



Искусственный
интеллект



Интернет вещей



Подрядчики

*На приказ № 21 ссылаются внутренние регламенты, ТЗ, акты
оценки эффективности — замена затрагивает весь пакет
документов*

Почему откладывать нельзя: ответственность уже ужесточена

1–3%

выручки — оборотный штраф
за повторную утечку

ст. 13.11 КоАП РФ, с 30.05.2025

до 500 млн ₽

верхняя граница оборотного
штрафа

ст. 13.11 КоАП РФ, с 30.05.2025

УК 272.1

уголовная ответственность за
незаконный оборот ПДн

с 11.12.2024

Новые требования не меняют ответственность, но меняют то, как оператор доказывает достаточность мер

Проект опубликован, но не принят — приказ № 21 продолжает действовать

24.07.2026

Проект приказа «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн»

до 08.08.2026

Общественное обсуждение на regulation.gov.ru (проект ID 169583)

01.09.2026

Заявленная в проекте дата вступления в силу — не наступила: приказ не зарегистрирован и не опубликован

25.08.2026

ФСТЭК России письменно: дата вступления в силу «будет скорректирована»

02

Анализ реформы

Что принципиально меняется и что придётся пересмотреть

От перечня мер — к риск-ориентированной модели

БЫЛО · приказ № 21

Жёсткий перечень мер по уровню защищённости

- Таблица ИАФ, УПД, ЗНИ... под свой УЗ
- Выбор = отметка галочками
- Обоснование почти не требуется

СТАЛО · проект

Оператор сам формирует состав мер

- Исходя из актуальных угроз, архитектуры и технологий ИС
- Содержание мер — по методическому документу ФСТЭК от 12.04.2026
- Состав мер закрепляется в политике обработки ПДн

Три шага выбора мер

01

Базовый набор

Определить базовые меры для уровня защищённости ИСПДн (по ПП РФ № 1119)



02

Адаптация

Скорректировать набор под архитектуру и используемые технологии: облака, контейнеры, API, ИИ



03

Верификация

Проверить достаточность против актуальных угроз и возможностей нарушителя; при необходимости дополнить или усилить меры

Можно выдохнуть: фундамент остаётся прежним



01

Уровни защищённости

УЗ-1...УЗ-4 по ПП РФ № 1119
— классификация систем
прежняя



02

Классы средств защиты

УЗ-1 — не ниже 4 класса, УЗ-2
— не ниже 5, УЗ-3/4 — 6 класс



03

Определение угроз

Обязательно. Отдельную
модель угроз оператор
разрабатывает по своему
решению

Новый состав: направления + меры

21

направление
реализации мер (п. 11)

Процессы: угрозы, конфигурации, уязвимости,
мониторинг, разработка, подрядчики, ГосСОПКА...

17

групп технических мер
(п. 12)

ИАФ, УПД, регистрация событий, виртуализация,
контейнеры, почта, веб, API, IoT...

Более 10 направлений — новые для ИСПДн. В приказе № 21 их не было как отдельных категорий: ИИ, контейнеры, API, IoT, почта, веб, DDoS, безопасная разработка, подрядчики, ГосСОПКА и др.

Новые направления: что защищать и что выстроить

ТЕХНОЛОГИИ · что защищать



Искусственный интеллект

Фильтрация запросов и ответов, контроль утечек ПДн



Контейнеры и оркестрация

Образы, реестры, среды оркестрации



API

Контроль схем запросов и интеграций



Интернет вещей

Устройства, входящие в инфраструктуру ИС



Электронная почта

Защита почтового контура



Веб-технологии

Веб-приложения и веб-сервисы

ПРОЦЕССЫ · что выстроить



Защита от DDoS

Атаки на отказ в обслуживании



Безопасная разработка ПО

Security by design для собственного ПО



Работа с подрядчиками

Требования к обработчикам, включая Узи



Взаимодействие с ГосСОПКА

Непрерывный обмен сведениями об инцидентах



Мониторинг ИБ

Выявление событий и инцидентов



Уязвимости и обновления

Управление уязвимостями и конфигурациями

Уровень зрелости защиты информации (Узи)

Когда оценивать (п. 9 проекта)



До начала обработки ПДн



Не реже 1 раза в 3 года



После компьютерного инцидента

Самостоятельно или с лицензиатом ФСТЭК по ТЗКИ.
Методика оценки утверждена ФСТЭК России 07.08.2026.

Рекомендуемые целевые уровни (Методика)

Система	Узи не ниже
ИСПДн УЗ-3 / УЗ-4	1
ИСПДн УЗ-2	2
ИСПДн УЗ-1	3

Шкала 0–4: нулевой · начальный · системный ·
контролируемый · верифицируемый. Оценка по 21
направлению.

Узи становится требованием к подрядчикам

01

Установить

Оператор сам задаёт требуемое значение Узи для лица, обрабатывающего ПДн по его поручению (п. 10 проекта)

02

Закрепить

Внести целевой Узи и порядок оценки в договор / поручение на обработку

03

Контролировать

Та же периодичность: до начала, не реже 1 раза в 3 года и внеочередно после инцидента у обработчика



Кого это касается в первую очередь

Облачные и SaaS-сервисы,
бухгалтерия и кадровый аутсорс

Три участка, на которых будет основной объём работ



Угрозы

- Актуализировать перечень угроз с учётом новых технологий
- Решить, сохранять ли модель угроз как документ
- Связать угрозы с выбором мер



Система защиты

- Разрыв-анализ по 21 направлению и 17 группам мер
- Новые зоны: ИИ, контейнеры, API, почта, веб
- Классы СЗИ — без изменений



Документация

- Обоснование выбора мер (3 шага)
- Политика обработки ПДн: состав мер без лишних деталей
- Отчёт об оценке Узи, договоры с обработчиками

ГЛАВНАЯ ПРАКТИЧЕСКАЯ БОЛЬ

**Раньше — формально скопировать таблицу.
Теперь — письменно обосновать свой выбор.**

Разрыв у большинства компаний будет не в наличии мер, а в способности их обосновать.

03

Разъяснения ФСТЭК России

Два письменных ответа на официальные запросы

ФСТЭК России, № 240/22/5799 от 25.08.2026



№ 240/22/5799

от 25.08.2026

Подпись: начальник 2
управления

Ответ на официальный запрос

1

Внеплановая оценка (оценка эффективности)

Не требуется при наличии документов по действующему приказу № 21

2

Дата вступления в силу

Будет скорректирована

3

Состав мер

Опора — методический документ ФСТЭК России от 12.04.2026

ФСТЭК России, № 240/22/6068 от 03.09.2026



№ 240/22/6068

от 03.09.2026

Ответ на дополнительные
вопросы после письма № 1

1

Заключённые договоры

ФСТЭК не планирует распространять действие приказа на работы по договорам, заключённым до его вступления в силу

2

Документирование Узи

Требования — в Методике от 07.08.2026 (документирование результатов — раздел VI)

04

Что делать уже сейчас

Кому паниковать рано, кому готовиться сегодня — и пошаговый план

Кому паниковать рано, кому готовиться уже сегодня

**Нет документов по оценке
эффективности**

Закрывать пробел в приоритете — по действующему приказу № 21

Готовиться сегодня

Есть обработчики ПДн

Инвентаризировать поручения, готовить требования к Узи

Готовиться сегодня

Документы по приказу № 21 есть

Начать разрыв-анализ по новым направлениям: ИИ, API, подрядчики

Планомерно

Договор на работы уже идёт

Зафиксировать дату договора.
Работы — по действующим требованиям

Паниковать рано

Подготовка до вступления приказа в силу

1



Аудит текущих мер

Что реализовано по приказу № 21, какие документы и оценки есть, кто обработчики

2



Разрыв-анализ

Сопоставить с 21 направлением и 17 группами мер, Узи — с целевым уровнем

3



Приоритизация

Сначала — актуальные угрозы, новые направления, подрядчики, а затем остальное

4



Актуализация документов

Обоснование мер, политика ПДн, договоры, отчёт по Узи

Цикл замыкается: оценка Узи → совершенствование мер → новая оценка (не реже 1 раза в 3 года).

Возможные ошибки — и как их избежать

ОШИБКА

КАК ИЗБЕЖАТЬ

- | ОШИБКА | КАК ИЗБЕЖАТЬ |
|---|---|
|  Переделывать уже сейчас |  Ориентироваться на финальный текст. № 21 пока действует |
|  Остановить текущие проекты по № 21 |  Довести до конца: документы по № 21 освобождают от внеплановой оценки |
|  Раскрыть лишнее в политике ПДн |  Указывать состав мер без технических деталей СЗИ |
|  Не зафиксировать дату договора |  Дата заключения — основание не применять новые требования |
|  Оценить Узи «на глаз» |  Отчёт по Методике: исходные данные, расчёт, план улучшений |

ВОПРОСЫ

Спасибо за внимание!