

b_152

После приказа №21: от теории к реализации

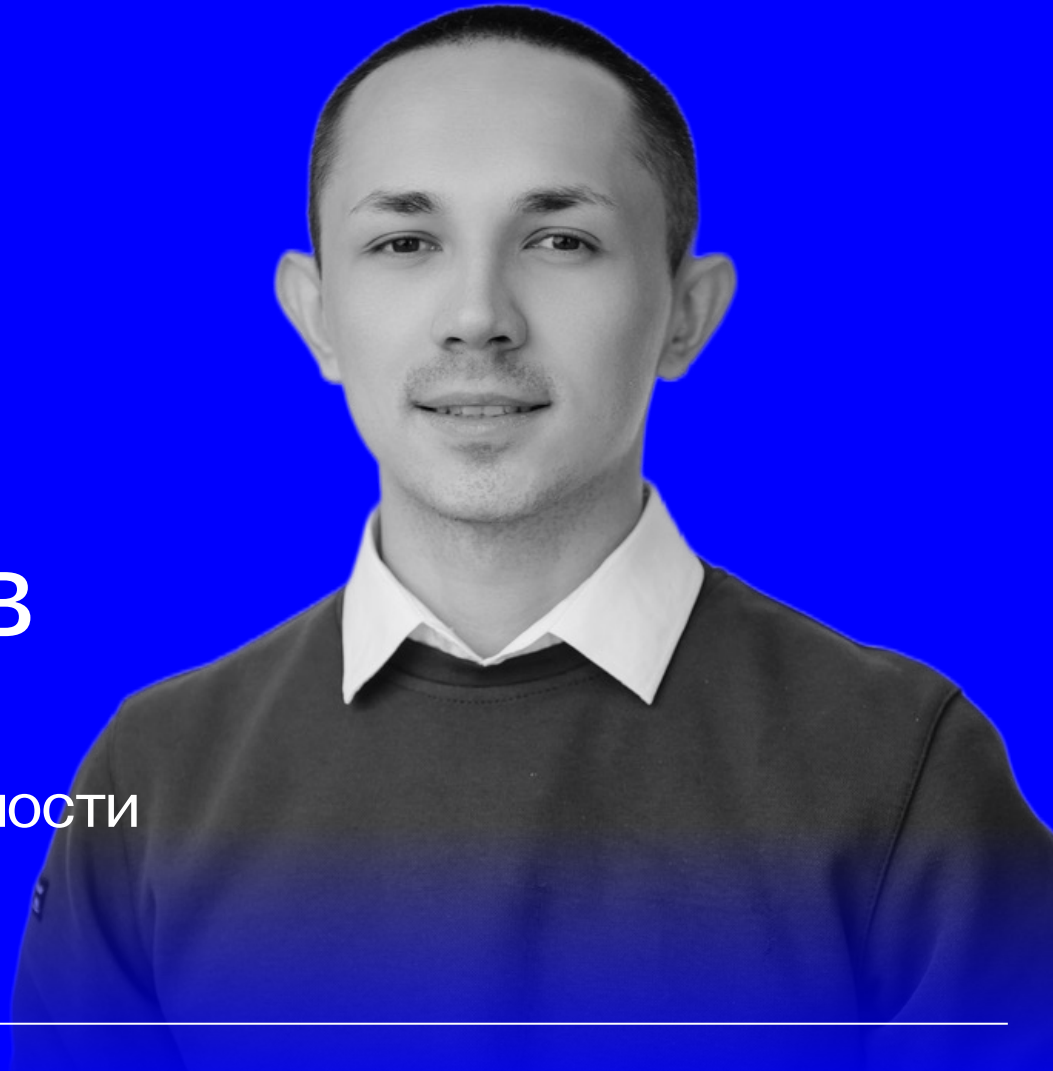
Оценка эффективности, уровень зрелости Узи и сценарий перехода для операторов персональных данных

АБИСС 2026 · Сессия «Персональные данные: от приказа до суда»

СПИКЕР

Егор Андюков

Старший специалист по
информационной безопасности



b_152

15 лет защиты персональных данных для лидеров рынка.

Мы делаем безопасность соблюдаемой, а бизнес — устойчивым

За 15 лет мы выстроили экспертный подход к Privacy и информационной безопасности.

Помогаем компаниям соответствовать ФЗ-152, 187-ФЗ и международным требованиям.

Обеспечиваем не просто соответствие, а безопасность, доверие и устойчивость бизнеса.



О ЧЁМ ПОГОВОРИМ

01 От теории к реализации

02 Как проходила оценка эффективности

03 Как она будет проходить

04 Расчёт уровня зрелости

05 Подготовка к первой ОЭ

ОТ ТЕОРИИ К РЕАЛИЗАЦИИ

Что меняется — разобрали в предыдущем докладе. Сейчас — как это подтвердить на практике

Предыдущий доклад: что меняется

Перечень мер → риск-ориентированная модель, новые направления, показатель Узи, разъяснения ФСТЭК



Этот доклад: как доказать

Порядок ОЭ «было → будет», ПМИ нового образца, расчёт Узи на цифрах, доказательная база для первой оценки

Мало обосновать выбор мер — на оценке придётся доказать, что они работают и процесс зрелый

ОЦЕНКА ЭФФЕКТИВНОСТИ ОСТАЁТСЯ ОБЯЗАТЕЛЬНОЙ

Техническое следствие письма ФСТЭК № 240/22/5799: что меняется в самой оценке

«...после вступления в силу проекта приказа ФСТЭК России оценка эффективности мер по обеспечению безопасности персональных данных должна проводиться в соответствии с действующими Составом и содержанием...»

Письмо ФСТЭК России № 240/22/5799 от 24.08.2026

ОЭ по приказу №21 уже есть

Внеплановая оценка после вступления нового приказа не требуется

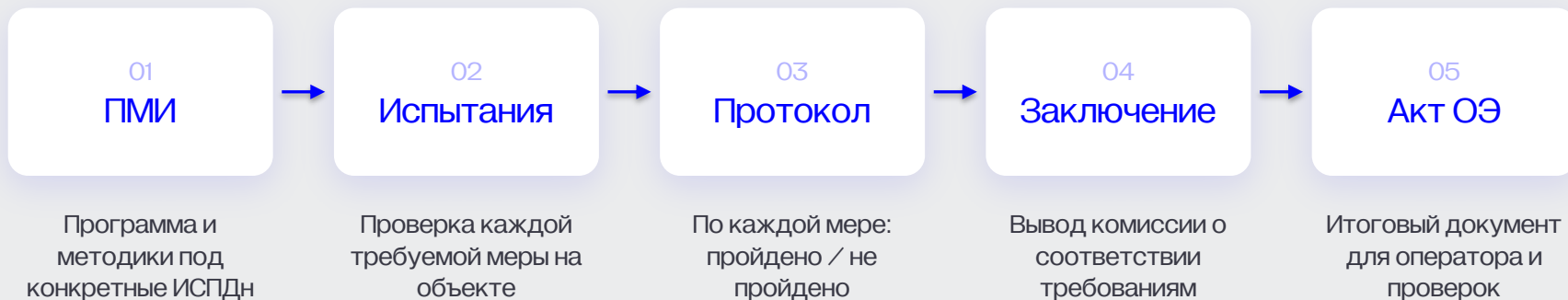
Следующая плановая ОЭ

Проводится уже по новому Составу и содержанию мер

Как было: Оценка эффективности по приказу №21

КАК БЫЛО: ПОРЯДОК ОЦЕНКИ ЭФФЕКТИВНОСТИ

По приказу №21 — так мы проводили ОЭ для каждого клиента



Важно: отдельного порядка ОЭ для ИСПДн не было — работали по аналогии с аттестацией (приказ ФСТЭК России №77 от 29.04.2021) и по методикам лицензиата

Что НЕ было критерием

Не пентест.

Что было критерием

Подтверждение, что каждая требуемая мера реализована

Настроено ли средство
защиты

Работает ли механизм

Есть ли документ, который
это закрепляет

Ограничение: результат бинарный — мера либо есть, либо нет. Регулярность процессов и квалификация людей в протокол не попадали

НА ПРАКТИКЕ: ПРОТОКОЛ МЕРА ЗА МЕРОЙ

Обезличенный проект: ИСПДн УЗ-3 / УЗ-4 в облачной инфраструктуре

≈ 70

листов ПМИ: методика
проверки каждой меры

≈ 20

листов протокола: результат
по каждой мере

≈ 20

позиций чек-листа:
настройки, сканирование,
формуляры, ЛНА

ФРАГМЕНТ ПРОТОКОЛА

ИАФ.1

Идентификация и аутентификация
пользователей

пройдено

УПД.2

Методы управления доступом

пройдено

РСБ.3

Сбор, запись и хранение событий

пройдено

АВЗ.1

Антивирусная защита

пройдено

АНЗ.1

Выявление и анализ уязвимостей

пройдено

ЗСВ.1

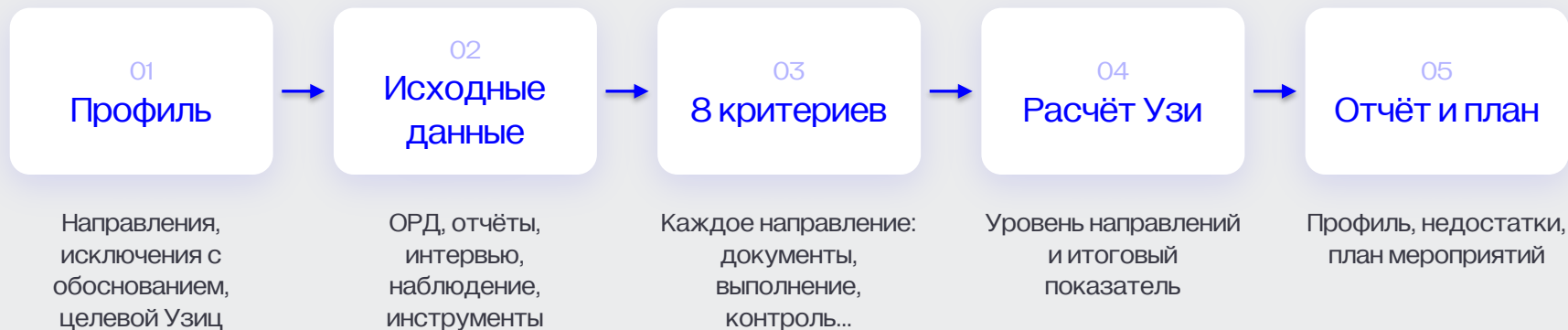
Защита среды виртуализации

пройдено

**Как будет: появление новой
оценки уровня зрелости**

КАК БУДЕТ: ПОРЯДОК ОЦЕНКИ ПО НОВЫМ ПРАВИЛАМ

Та же логика «программа → проверка → отчёт», но результат — уровень зрелости



Результат: не «пройдено / не пройдено», а уровень 0—4 по каждому направлению и итоговый Узи против целевого Узиц

ОЦЕНКА ЭФФЕКТИВНОСТИ: БЫЛО → БУДЕТ

Письмо ФСТЭК № 240/22/6068: результаты — по Методике уровня зрелости от 07.08.2026

ПО ПРИКАЗУ №21

ПО НОВЫМ ПРАВИЛАМ

Методология

По аналогии с аттестацией, методики лицензиата



Единая методика ФСТЭК

Что проверяем

Перечень мер под УЗ



Обоснованные меры и направления деятельности

Критерий

Пройдено / не пройдено



Уровень 0–4 по 8 критериям против Узиц

Доказательства

Скриншоты, отчёт сканера, формуляры



+ интервью, наблюдение, плановые отчёты

Кто проводит

Оператор или лицензиат



Внутренняя оценка или внешняя — лицензиат

Результат

Протокол и заключение



Отчёт: профиль, недостатки, план мероприятий

ПРОГРАММА И МЕТОДИКИ НОВОГО ОБРАЗЦА

Инструментальная проверка остаётся, но становится доказательством зрелости процесса

01

Профиль зрелости

Направления, исключения с обоснованием, целевой Узиц

02

Исходные данные

ОРД, отчёты, интервью, наблюдение, данные инструментов

03

Методы

Документальный, интервью, наблюдение, инструментальный

04

Проверка направлений

Каждое направление — по 8 критериям с доказательствами

05

Инструментальная часть

Настройки СЗИ и сканирование — как доказательства

06

Расчёт и отчёт

Узи по направлениям, итог, диаграмма, план мероприятий

ПРИМЕР: НАПРАВЛЕНИЕ «УПРАВЛЕНИЕ УЯЗВИМОСТЯМИ»

Как одно направление выглядит в новой ПМИ

Критерий	Вес w	Что проверяем и чем подтверждаем
Документирование	0,15	Регламент утверждён, доведён, актуализируется
Выполнение	0,20	Сканирование по графику, сроки устранения соблюдаются
Инструменты	0,10	Сертифицированный сканер, учёт уязвимостей в системе
Квалификация	0,10	Опыт исполнителей более года и (или) сертификаты
Контроль	0,15	Плановые проверки исполнения регламента
Обучение	0,10	Программа обучения для администраторов
Внешний аудит	0,10	Внешние оценки по графику, результаты используются
Актуализация	0,10	Улучшения процесса вносятся по плану

Шкала: а = 0 / 0,5 / 1 по каждому критерию (для «Обучения» есть 0,3). Веса — по таблице 2 Методики

Уровень зрелости Узи: расчёт на практике

КАК СЧИТАТЬ УЗИ

Шкала 0—4 и целевые уровни — в предыдущем докладе. Здесь — как получить число

Порядок расчёта

- 1 Профиль**
До 21 направления, неприменимое исключаем с обоснованием
- 2 8 критериев**
Для каждого: $D = w \cdot a$
- 3 Уровень направления Y_k**
Сумма R_{zn} + минимумы по каждому критерию
- 4 Итоговый Узи**
Сводим направления и сравниваем с Узиц

Формулы Методики

$$D = w \cdot a$$

значение критерия (п. 28)

$$R_{zn} = \sum D$$

итог по направлению (п. 29)

$$Узи = \sum (k \cdot Y_k) / \sum k$$

итоговый уровень (п. 31)

РАСЧЁТ НА ПРИМЕРЕ

«Управление уязвимостями»: цифры условные, для иллюстрации

Критерий	a	w	D
Документирование	1	0,15	0,150
Выполнение	0,5	0,20	0,100
Инструменты	1	0,10	0,100
Квалификация	0,5	0,10	0,050
Контроль	0,5	0,15	0,075
Обучение	0,3	0,10	0,030
Внешний аудит	0	0,10	0,000
Актуализация	0,5	0,10	0,050
Рзн			0,555

Итог

$Y_k = 2$

системный

Рзн = 0,555 — выше порога уровня 2 (0,35), все минимумы выполнены

До уровня 3 не хватает: «Выполнение» должно быть 0,20, «Контроль» — 0,15

Вывод: сумма высокая, но уровень держат самые слабые критерии

ПОДВОДНЫЕ КАМНИ МЕТОДИКИ

По тексту проекта Методики — сверьте с утверждённой редакцией от 07.08.2026

Вес направления = его номер

В п. 31 вес — порядковый номер к. «Контроль уровня защищённости» (№21) весит в 21 раз больше «Организации и управления» (№1)

«Дыра» в шкале

Уровень 0 — $R_{зн} < 0,2$, уровень 1 — от 0,225. Значения между ними не попадают ни в один уровень

Нет материалов — ноль

Если подразделение не представило документы, направлению присваивается нулевое значение (п. 23)

Независимость оценки

При внутренней оценке специалист не оценивает результаты собственной работы (п. 21)

КАЛЬКУЛЯТОР УЗИ

Чтобы не считать вручную по 21 направлению и 8 критериям

Что внутри: профиль направлений, 8 критериев с весами, проверка минимумов уровней и итоговый показатель

Результат: текущий Узи по каждому направлению и разрыв до целевого Узиц

Как получить: напишите нам — проконсультируем



t.me/b152privacy

Подготовка к первой оценке по новым правилам

ДОКАЗАТЕЛЬНАЯ БАЗА: ЧТО НАЧАТЬ КОПИТЬ СЕЙЧАС

Каждый из 8 критериев подтверждается документом — без него балл равен нулю

Документирование

Регламенты с листами ознакомления и историей изменений

Выполнение

Журналы, отчёты сканирования, заявки — по графику и с датами

Инструменты

Перечень средств с привязкой к процессам, выгрузки из них

Квалификация

Сертификаты и подтверждение опыта исполнителей

Контроль

План и протоколы внутренних проверок

Обучение

Программа, списки прошедших, результаты тестирования

Внешний аудит

График внешних оценок, отчёты, принятые меры

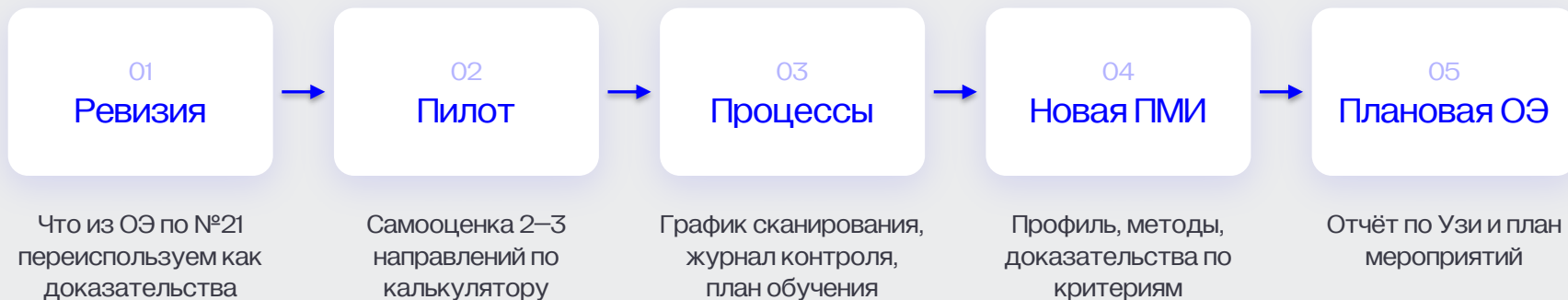
Актуализация

План улучшений и отметки о выполнении

Правило: непредставленные материалы оцениваются в 0 (п. 23 Методики) — копить надо до оценки, а не во время

ПОДГОТОВКА К ПЕРВОЙ ОЭ ПО НОВЫМ ПРАВИЛАМ

Технический порядок действий — от того, что уже есть по приказу №21



Важно: ОЭ по приказу №21 сейчас освобождает только от внеплановой оценки — к первой плановой ОЭ по новым правилам доказательную базу придётся собрать заново

Q&A

ВАШИ ВОПРОСЫ?

Спасибо!

b_152



САЙТ

b-152.ru



TELEGRAM

@ b152privacy



TELEGRAM

Чат экспертов

info@b-152.ru

+7 (499) 372-06-52