

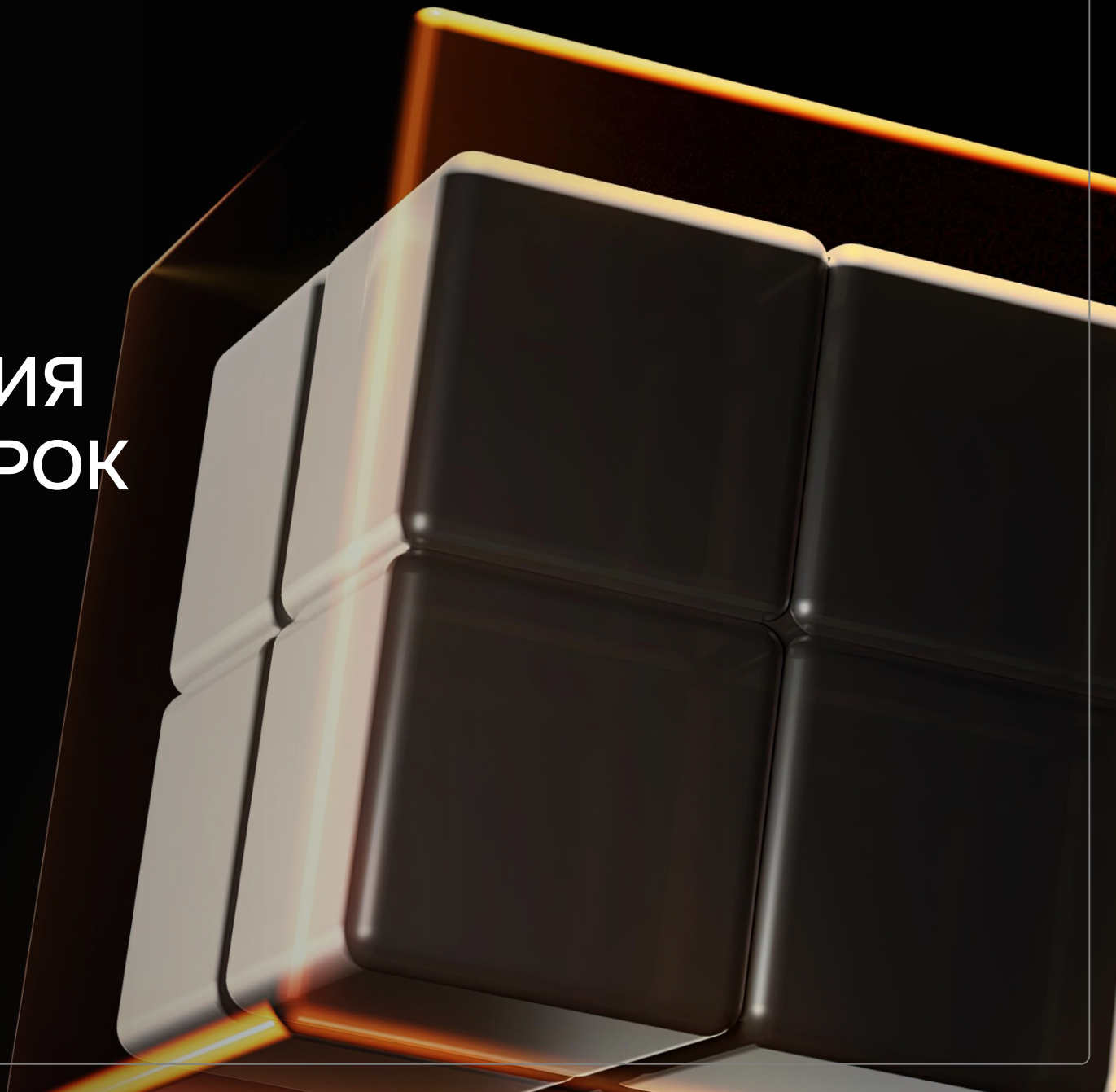


ЦЕНТР  
КИБЕРБЕЗОПАСНОСТИ

# СОВРЕМЕННЫЕ РЕШЕНИЯ ДЛЯ ПРОЦЕССА ПРОВЕРОК СООТВЕТСТВИЯ ТРЕБОВАНИЯМ ИБ

**Глеб Дворников**

Менеджер продукта УЦСБ



# Проверка соответствия требованиям

## КОНТРОЛЬ В ИБ

— оценка соответствия организационных и технических мер установленным требованиям информационной безопасности

## ЦЕЛЬ ПРОВЕДЕНИЯ

— подтвердить соответствие законодательным требованиям ИБ, а также оценить способность инфраструктуры противостоять кибератакам

# Проблемы, с которыми сталкиваются организации в рамках контроля соответствия требованиям ИБ



МНОГОЧИСЛЕННОСТЬ  
И ТЕРРИТОРИАЛЬНАЯ  
РАСПРЕДЕЛЕННОСТЬ  
ПРОВЕРЯЕМЫХ ОБЪЕКТОВ



ОГРАНИЧЕННЫЕ СРОКИ  
ДЛЯ ВЫЕЗДНОЙ  
ПРОВЕРКИ ОБЪЕКТОВ



ВЫСОКАЯ СТОИМОСТЬ  
ПРИВЛЕЧЕНИЯ ЭКСПЕРТОВ



ОГРАНИЧЕННЫЕ РЕСУРСЫ  
ДЛЯ ВЫЕЗДНОЙ ПРОВЕРКИ  
ОБЪЕКТОВ



ИЗМЕНЧИВОСТЬ  
И БОЛЬШОЙ ОБЪЕМ  
ТРЕБОВАНИЙ НПА



ОТСУТСТВИЕ ЕДИНЫХ  
МЕТОДИК И ШАБЛОНОВ  
ДЛЯ ПРОВЕРКИ

# Какие инструменты обычно используют для проведения аудита

**1**

## АНАЛИЗ ДОКУМЕНТАЦИИ

- ОРД (политики, регламенты, приказы и другие ЛНА)
- ЭД на Объект КИИ
- ЭД на Системы безопасности КИИ

**2**

## АНАЛИЗ СРЗИ

- Конфигурации встроенных СрЗИ
- Конфигурации наложенных СрЗИ

**3**

## EXCEL - ТАБЛИЦА

- Оценка организации работ по обеспечению безопасности объектов КИИ
- Оценка защищенности объекта КИИ

# Внутренний аудит



## Задача

Автоматизировать и упростить внутренний аудит соответствия требованиям ИБ



# Решения для автоматизации аудита

---

**1**

**Организационная проверка**

---

**2**

**Техническая проверка**

---

**3**





**Ретроспективный анализ проверок**




---

# Организационная проверка

- 1 Перечень оцениваемых процессов, подпроцессов и требований к обеспечению ИБ
- 2 Свидетельства внутренней оценки реализации требований
- 3 Значения весовых коэффициентов для процессов, подпроцессов и требований
- 4 Расчет значений показателей оценок реализации процессов, подпроцессов и требований к обеспечения ИБ

# Анализ требований НПА

-  **Федеральный закон РФ от 26.07.2017 № 187-ФЗ**  
«О безопасности критической информационной инфраструктуры Российской Федерации»
-  **Приказ ФСТЭК России № 235**  
«Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»
-  **Приказ ФСТЭК России № 239**  
«Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»
-  **Постановление Правительства РФ от 08.02.2018 № 127**  
«Об утверждении правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений»











-  **Приказ ФСБ России от 19.06.2019 № 282**  
«Об утверждении порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации»
-  **Приказ ФСБ России от 24.07.2018 № 367**  
«Об утверждении перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»
-  **Постановление Правительства РФ от 17.02.2018 № 162**  
«Об утверждении правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»



# Выделены направления оценки соответствий по процессам

- |   |   |   |   |
|---|---|---|---|
| 1 | Категорирование объектов КИИ  | 6 | Обнаружение компьютерных инцидентов и реагирование на них |
| 2 | Организационно-распорядительное и нормативное обеспечение безопасности объектов КИИ | 7 | Выполнение требований нормативно-правовых актов           |
| 3 | Создание сил обеспечения безопасности объектов КИИ                                  | 8 | Обеспечение безопасности объекта КИИ с использованием ТС  |
| 4 | Управление системой обеспечения безопасности объектов КИИ                           | 9 | Обеспечение физической безопасности объекта КИИ           |
| 5 | Организация контроля выполнения требований  |   |   |

# Перечень документов с используемыми требованиями

-  **Федеральный закон РФ № 152-ФЗ**  
«Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»
-  **Постановление Правительства РФ № 1119**  
Требования к защите ПДн в ИСПДн, уровни защищённости и внутренний контроль не реже 1 раза в 3 года
-  **Приказ ФСТЭК России № 21**  
Состав и содержание организационных и технических мер защиты ПДн для каждого уровня по ПП-1119
-  **Приказ ФСБ России № 378**  
Меры по защите ПДн при использовании СКЗИ (криптографии) в ИСПДн
-  **Приказ Роскомнадзора от 30.05.2017 № 94**  
«Об утверждении методических рекомендаций по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения»
-  **Приказ Роскомнадзора от 14.11.2022 № 187**  
«Об утверждении Порядка и условий взаимодействия Роскомнадзора с операторами в рамках ведения реестра учета инцидентов в области персональных данных»
-  **Постановление Правительства РФ № 687**  
Особенности обработки ПДн без использования средств автоматизации
-  **Постановление Правительства РФ № 512**  
Требования к материальным носителям биометрических ПДн и технологиям хранения вне ИСПДн
-  **Постановление Правительства РФ от 17.02.2018 № 162**  
«Об утверждении правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»
-  **Приказ Федерального агентства правительственной связи и информации при Президенте РФ от 13.06.2001 № 152**  
«Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»

# Направления оценки соответствий по процессам

1

Классификация ПДн и определение уровня защищенности

5

Поручение и передача ПДн третьим лицам

2

Поиск актуальных угроз и выбор мер защиты ИСПДн

6

Установка средств защиты информации, в том числе СКЗИ

3

Организационно-распорядительная документация в области обработки и обеспечения безопасности ПДн

7

Обнаружение и реагирование на утечки ПДн

4

Назначение лиц, ответственных за обработку и обеспечение безопасности ПДн

8

Оценка эффективности

# Методика оценки уровня безопасности объекта КИИ

01.

**Аудитор выставляет оценку реализации требования**

- Выполняется
- Не выполняется

02.

**Расчет весового коэффициента подпроцесса**

- Средневзвешенное значение оценок входящих требований

03.

**Расчет весового коэффициента процесса**

- Средневзвешенное значение оценок входящих подпроцессов

04.

**Расчет итоговой оценки уровня безопасности**

- Средневзвешенное значение оценок входящих процессов

## Расчет весового коэффициента

$$E_{pp}^k = \frac{\sum_j (v_i^k \times w_i^k)}{\sum_j w_i^k}$$

- $E_{pp}$  – числовое значение оценки подпроцесса
- $V$  – числовая оценка выполнения требования
- $W$  – весовой коэффициент требования (равен 1)
- $k$  – порядковый номер процесса;
- $i$  – порядковый номер подпроцесса;
- $j$  – порядковый номер требования по безопасности

# Формирование отчетной документации

- Генерация протокола контроля выполнения требований



Протокол  
контроля выполнения требований в области обеспечения  
безопасности объектов КИИ

---

---

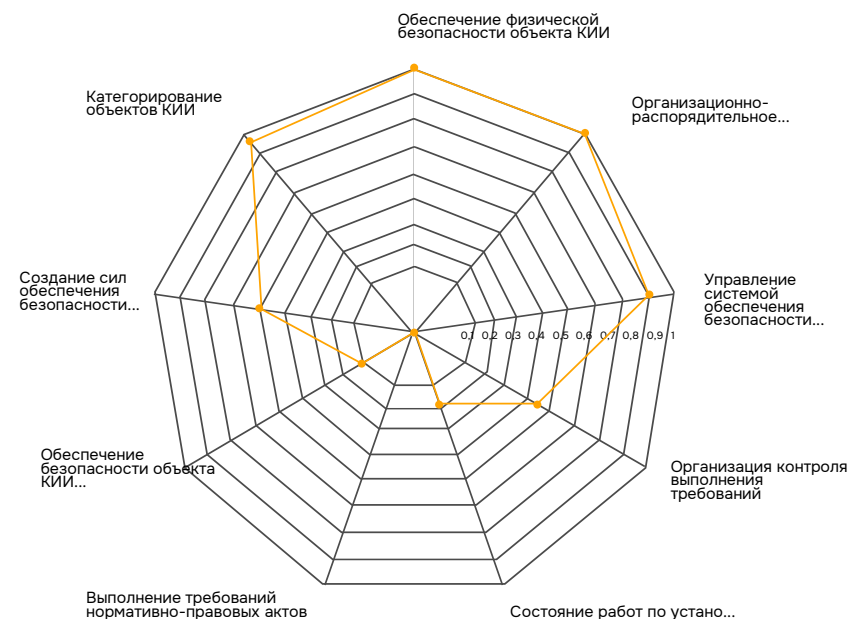
---

---

---

---

## УРОВЕНЬ РЕАЛИЗАЦИИ ТРЕБОВАНИЙ



выполнено требований - 20

не выполнено требований - 0

# Технические проверки

- 1** Сканеры безопасности
- 2** Подключение к маршрутизатору сети объекта защиты
- 3** Сканирование сети: сбор информации через СРЗИ
- 4** Проверка технических мер на соответствие законодательным требованиям

# Проверка технических мер

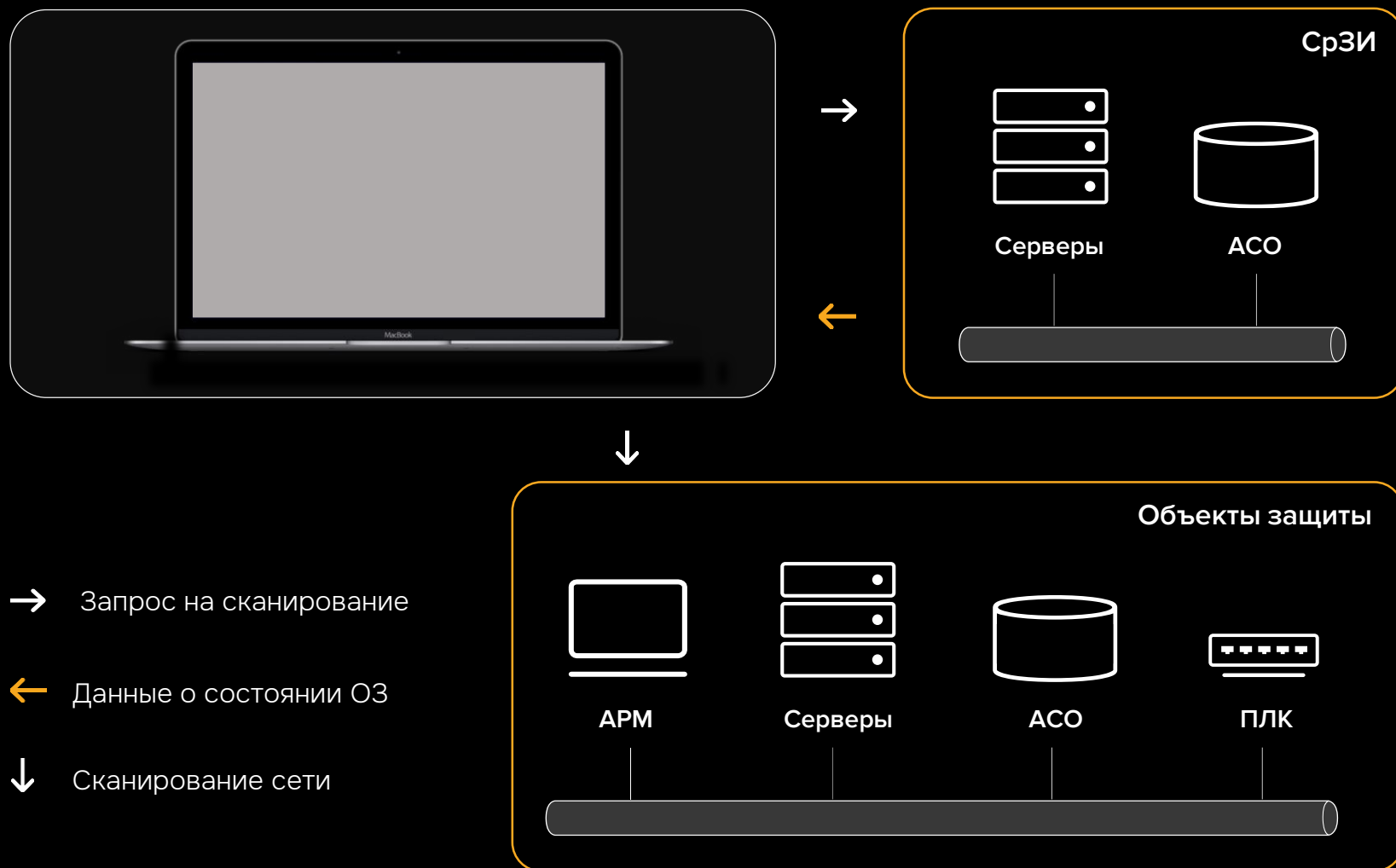


## Пример

Проверка парольной политики на соответствие: ИАФ 1



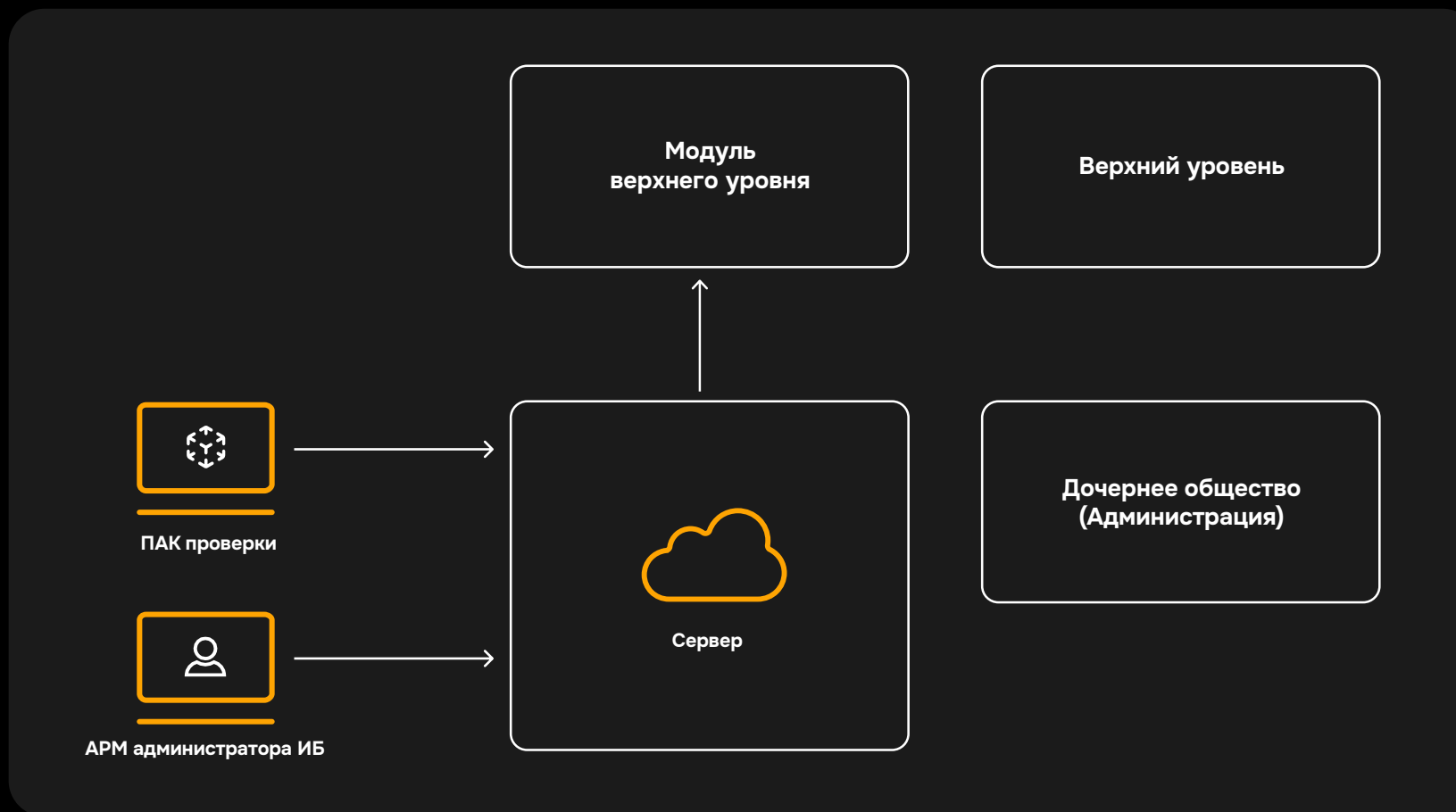
# Технические проверки



# Ретроспективный анализ

- 1** Сравнительный анализ изменений в реализации мер безопасности одного и того же объекта в разные временные периоды внутренней проверки
- 2** Отслеживание изменений уровня защищенности конкретного объекта: устранение выявленных ранее недостатков, улучшения или ухудшения функций безопасности

# Централизованный сбор информации с последующей генерацией отчетов





# Ключевые преимущества автоматизации аудита



Проведения аудита крупной  
распределенной сети объектов  
в сжатые сроки



Увеличение скорости  
проверки



Создание единого шаблона  
проверок



Снижение нагрузки персонала  
при проведении ручных проверок



Снижение расходов на аудит



Автообновляемые шаблоны  
по изменениям в НПА



ЦЕНТР  
КИБЕРБЕЗОПАСНОСТИ

# СПАСИБО ЗА ВНИМАНИЕ! ВОПРОСЫ?

**Глеб Дворников**

Менеджер продукта УЦСБ

Узнайте больше о нашем продукте  
для автоматизации аудита



[sec.USSC.ru](https://sec.USSC.ru)