

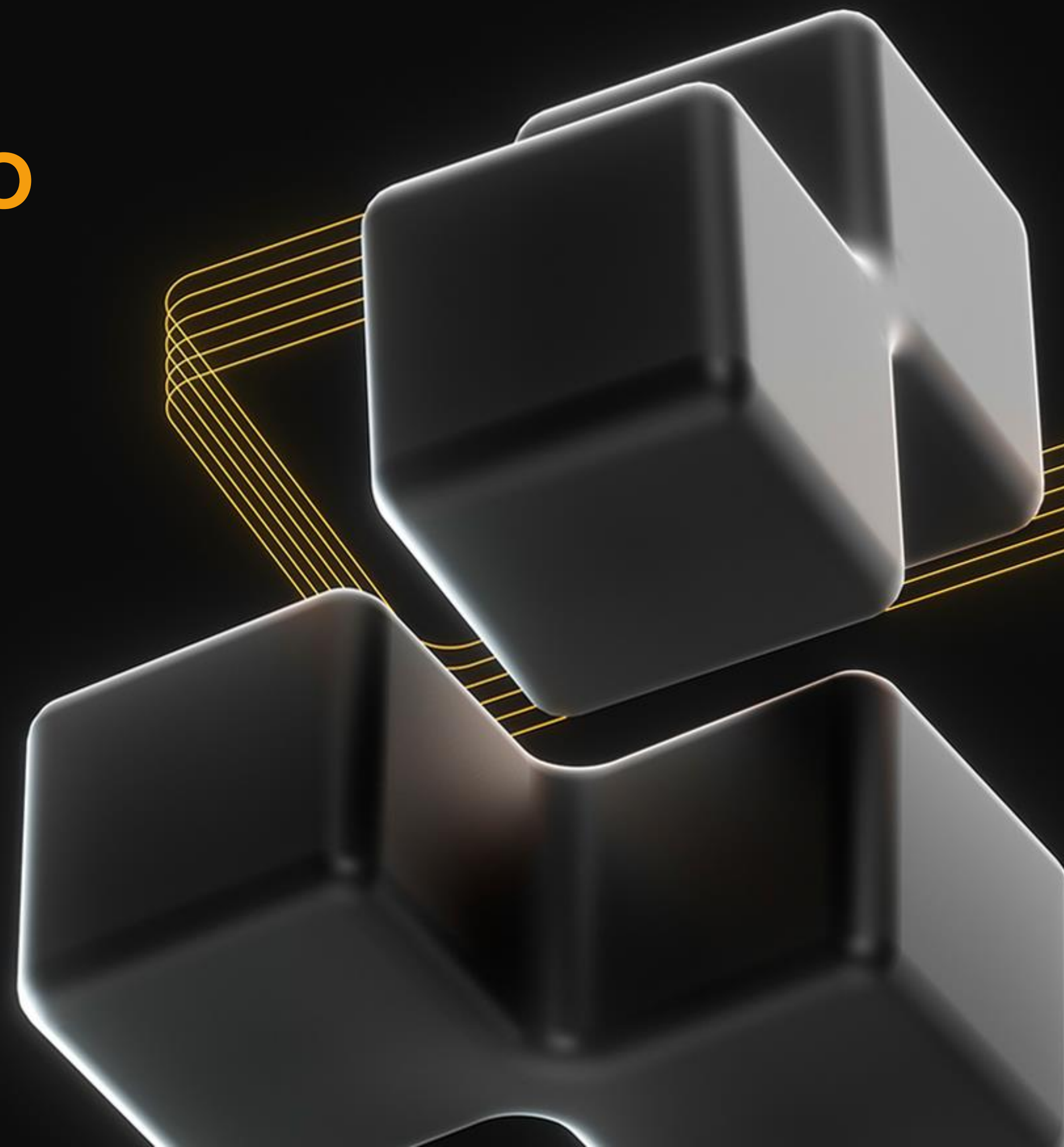


СЛОЖНОСТИ ВНУТРЕННЕГО КОНТРОЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОБЪЕКТОВ КИИ

Как с ними справляться?

Анастасия Федоренко

Руководитель направления «Автоматизация ИБ»



01. Знакомство

Анастасия Федоренко

- Руководитель направления «Автоматизация ИБ» в Аналитическом центре УЦСБ
- Автоматизируем бизнес-процессы ИБ с помощью систем SOAR/IRP, SGRC, Security Awareness
- Обладаю опытом проектирования и внедрения систем обеспечения безопасности АСУ ТП
- Опыт в ИБ ~ 10 лет



**Уральский центр
систем безопасности
(УЦСБ)**

> 16

лет на рынке

> 900

профессионалов в штате

> 1500

завершенных проектов

03. Введение

Внутренний контроль

— внутренняя оценка организации работ по обеспечению безопасности объектов КИИ и эффективности принимаемых организационных и технических мер*

Цель проведения внутреннего контроля

— определение способности созданных систем безопасности обеспечивать устойчивое функционирование объектов КИИ при проведении в отношении них компьютерных атак

Контроль проводится не реже, чем раз в 3 года.
Периодичность контроля определяется руководителем субъекта КИИ *

***Приказ ФСТЭК России № 235** «Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»

04. А в чем же сложность?

Большой объем требований НПА,
регулирующих защиту
объектов КИИ



Вариативность подходов
к реализации требований
безопасности



Вариативность подходов
к контролю реализации
требований безопасности



Аудитор ИБ



Многочисленность
проверяемых объектов КИИ

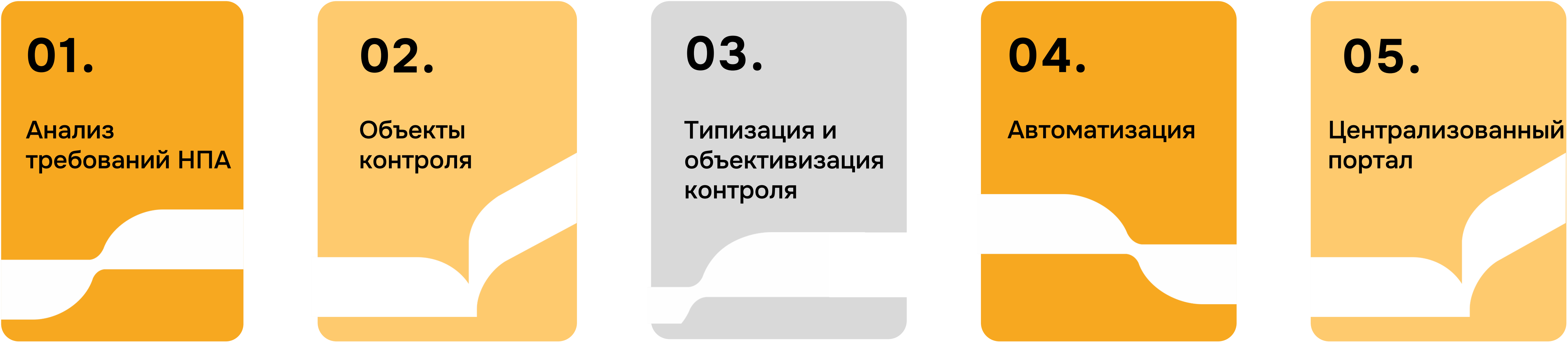


Ограниченные сроки проверки



Ограниченные ресурсы

05. **Путь оптимизации**



06. 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»

07. Объекты контроля

01.

Документация
на объекты КИИ

02.

Персонал

03.

Объекты КИИ

04.

Системы обеспечения
безопасности объектов
КИИ

05.

Физическая безопасность
объектов КИИ

08. Объекты контроля

01.

Документация на объекты КИИ*

- Категорирование объектов КИИ (сведения, порядок, комиссия)
- Регламентация правил и процедур обеспечения безопасности объектов КИИ
- Техническая документация на объекты КИИ
- Техническая документация на системы безопасности объектов КИИ
- Оценка соответствия СрЗИ требованиям по безопасности
- Квалификация лиц, ответственных за обеспечение безопасности объектов КИИ, корректность назначения
- Должностные инструкции



* Постановление Правительства РФ от 08.02.2018 № 127
Приказ ФСТЭК России № 235
Приказ ФСТЭК России № 239

09. Объекты контроля

02.

Персонал *

Лица, ответственные за обеспечение безопасности ОКИИ

- знания
- осведомленность
- функции и обязанности



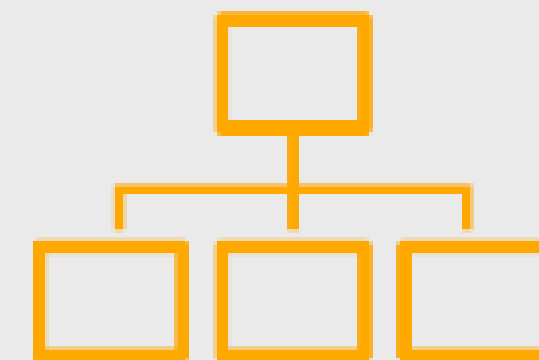
* Приказ ФСТЭК России № 235
Приказ ФСТЭК России № 239

10. Объекты контроля

03.

Объекты КИИ*

- Компоненты объектов КИИ
средства вычислительной техники, сетевое оборудование,
программируемые логические контроллеры, программное обеспечение
- Конфигурация компонентов объектов КИИ
- Архитектура объектов КИИ



* Приказ ФСТЭК России № 239

11. Объекты контроля

04.

Системы обеспечения безопасности объектов КИИ*

- Технические меры по обеспечению безопасности ОКИИ
- СрЗИ (в том числе, встроенные)
- Конфигурация системы обеспечения безопасности ОКИИ
- Защищенность



* Приказ ФСТЭК России № 239

12. Объекты контроля

05.

Физическая безопасность объектов КИИ

Физический доступ к компонентам ОКИИ

контролируемая зона, внутриобъектовый и пропускной режим,
размещение компонентов ОКИИ



* Приказ ФСТЭК России № 239

13. Типизация и объективизация контроля

01.

Матрица требований

- Перечень установленных требований НПА
- Единые критерии реализации требований НПА
- Единые критерии контроля реализации требований НПА

02.

Опросный лист аудитора ИБ

- Проверка всех требований НПА
- Единые критерии контроля реализации требований НПА
- Единые результаты оценки
- Подтверждающие свидетельства*

* ГОСТ Р ИСО 19011-2021 «Оценка соответствия. Руководящие указания по проведению аудита систем менеджмента»

14. Типизация и объективизация контроля

01.

Матрица требований

ИАФ.1 Идентификация и аутентификация пользователей и инициируемых ими процессов*

КРИТЕРИИ РЕАЛИЗАЦИИ

- Наличие логина/пароля у каждого пользователя системы
- Для всех процессов указаны пользователи, их запустившие

КРИТЕРИИ КОНТРОЛЯ ОС WINDOWS

- Параметр DefaultPassword отсутствует в редакторе реестра
- Минимальная длина пароля отлична от нуля
- Список пользователей, запускавших процессы совпадает со списком залогинившихся

КРИТЕРИИ КОНТРОЛЯ ОС ASTRA LINUX

- password*pam_unix.so* в файле /etc/pam.d/common-password присутствует. Значение параметра minlen ненулевое
- В ps aux запущенных процессов пользователи совпадают с теми, что найдены в /etc/passwd

* Приказ ФСТЭК России № 239

15. Типизация и объективизация контроля

01.

Матрица требований

п. 11 ПП РФ № 127. Для проведения категорирования решением руководителя субъекта КИИ создается постоянно действующая комиссия по категорированию...*

КРИТЕРИИ РЕАЛИЗАЦИИ

- В организации создана комиссия по категорированию объектов КИИ (решением руководителя субъекта КИИ)
- Состав комиссии актуален на момент оценки и соответствует требованиям

КРИТЕРИИ КОНТРОЛЯ

- Присутствует утвержденный Приказ о создании комиссии по категорированию объектов КИИ
- Состав комиссии актуальный (сотрудники состоят в штате организации, дата актуальная)
- Состав комиссии по категорированию объектов КИИ включает работников...

* Постановление Правительства РФ от 08.02.2018 № 127

16.

Типизация и объективизация контроля

02.

Опросный лист аудитора ИБ

Требование	Результат оценки	Критерии контроля	Результат оценки	Свидетельство
п. 11 ПП РФ № 127 *	Выполняется частично	Утвержденный приказ руководителя субъекта КИИ о создании комиссии	Да	Скан приказа о создании комиссии по категорированию объектов КИИ 
		Состав комиссии актуальный	Нет	
		Состав комиссии включает работников...	Да	

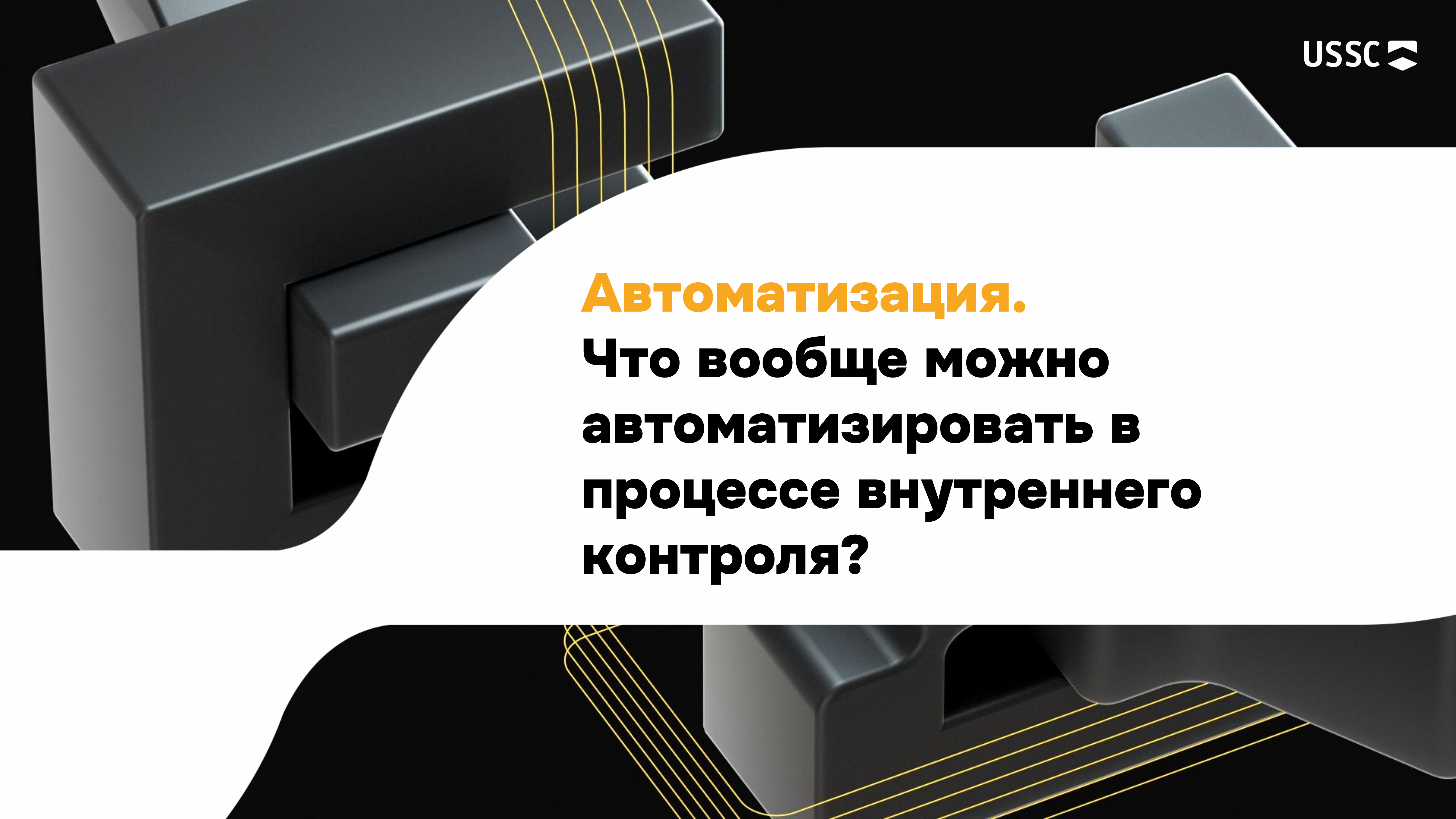
* Постановление Правительства РФ от 08.02.2018 № 127

17. Сколько это займет времени?



18. **Сколько это займет времени?**





Автоматизация.
**Что вообще можно
автоматизировать в
процессе внутреннего
контроля?**

19. Автоматизация

01.

Заполнение опросного листа
аудитора ИБ

02.

Контроль технических мер
безопасности

20. Автоматизация

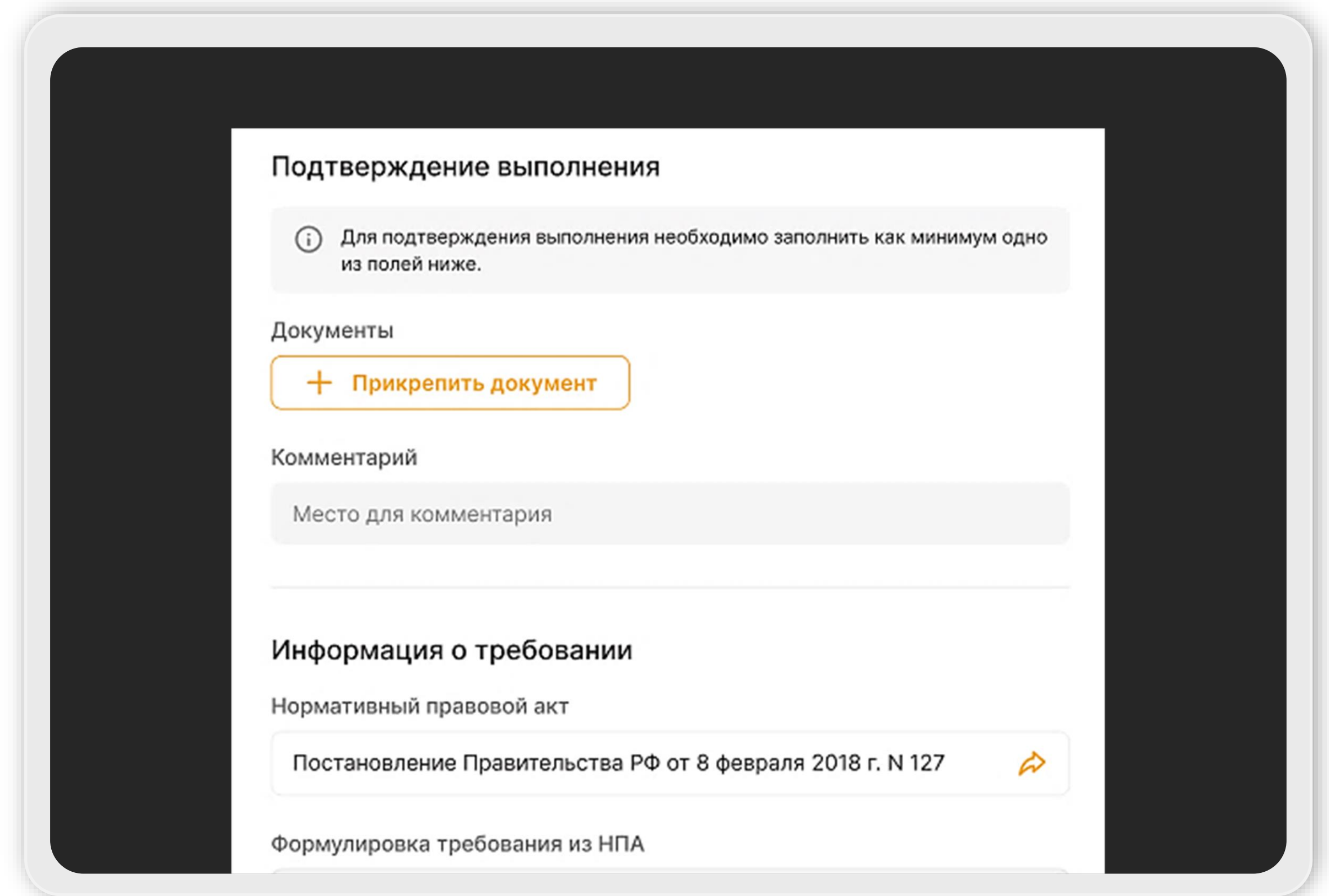
01. Заполнение опросного листа аудитора ИБ

- Визуализация требований по группам проверки
- Ответы из выпадающего списка «да/нет»
- Автоматический расчет общего результата
«Выполняется/Не выполняется/Выполняется частично»
- Автоматическое отслеживание полноты заполнения опросного листа
- Автоматическое формирование акта внутренней проверки

21. Автоматизация

01. Заполнение опросного листа аудитора ИБ

- Подкрепление свидетельств
- Контроль подтверждения результата
- НПА в быстром доступе из каждого пункта требования



Подтверждение выполнения

 Для подтверждения выполнения необходимо заполнить как минимум одно из полей ниже.

Документы

 Прикрепить документ

Комментарий

Место для комментария

Информация о требовании

Нормативный правовой акт

Постановление Правительства РФ от 8 февраля 2018 г. N 127 

Формулировка требования из НПА

22. Автоматизация

01. Заполнение опросного листа аудитора ИБ

Заполнение опросного листа

Завершить заполнение

Требование 1

5/10 требований

Создание в организации постоянно действующей комиссии по категорированию объектов КИИ (решением руководителя субъекта КИИ). Актуальность состава комиссии и его соответствие требованиям п.11, 13 ППр 127

Требование 1.1

Создание в организации постоянно действующей комиссии по категорированию объектов КИИ (решением руководителя субъекта КИИ). Актуальность состава комиссии и его соответствие требованиям п.11, 13 ППр 127

Да

Требование 1.2

Состав постоянно действующей технической комиссии по категорированию объектов КИИ соответствует требованиям п.11 ППр 127

Нет

Требование 1.3

В состав комиссии входит руководитель субъекта критической информационной инфраструктуры или уполномоченное им лицо

Требование 1

Сохранить

Результат

Результат рассчитан автоматически на основе результатов, полученных из вложенных подтребований.

Выполняется частично

Подтверждение выполнения

Для подтверждения выполнения необходимо заполнить как минимум одно из полей ниже.

Документы

Прикрепить документ

Комментарий

Место для комментария

23. Автоматизация

02. Контроль технических мер безопасности *

- Автоматический анализ уязвимостей и их устранение
- Автоматический анализ наличия МЭ в сети ОКИИ

Без интеграции с СрЗИ

* Приказ ФСТЭК России № 239

23. Автоматизация

02. Контроль технических мер безопасности *

- Автоматический анализ уязвимостей и их устранение
- Автоматический анализ наличия МЭ в сети ОКИИ

Без интеграции с СрЗИ

- Автоматизированный анализ конфигурации компонентов ОКИИ
- Автоматизированный анализ корректности функционирования СрЗИ ОКИИ



Интеграция с СрЗИ

* Приказ ФСТЭК России № 239

24. Автоматизация

02. Контроль технических мер безопасности

- Автоматический расчет оценки реализации меры «Выполняется/Не выполняется/Выполняется частично»
- Автоматическое формирование акта внутренней проверки

ИАФ.1 Идентификация и аутентификация пользователей и инициируемых ими процессов

Результаты

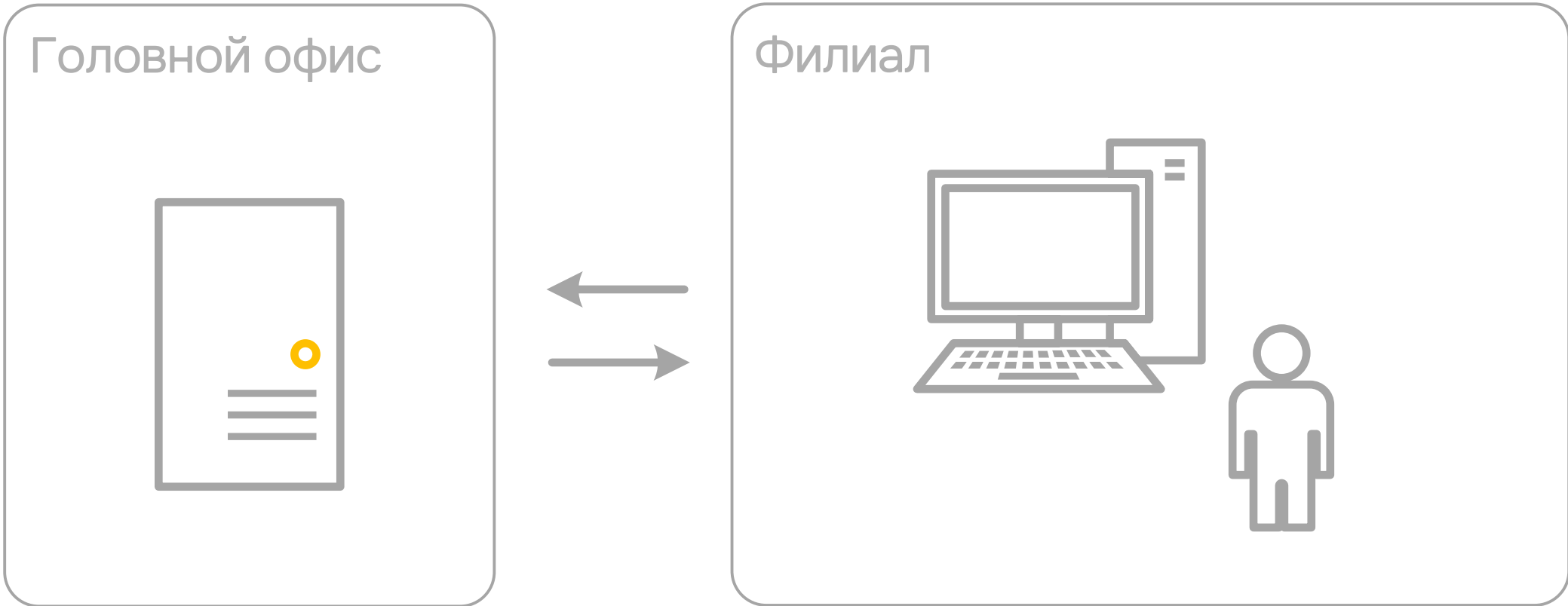
Методы проверки

Не выполняется

Имя устройства	IP-адреса	MAC-адреса	Параметр DefaultPassword	Минимальная длина пароля	Результат
APM SCADA 2			Параметр DefaultPassword не удалён	Минимальная длина пароля равна 0	Не выполняется
Сервер OPC 2			Параметр DefaultPassword не удалён	Минимальная длина пароля равна 0	Не выполняется

25. Централизованный портал

Единое пространство, позволяющее сохранить унификацию процессов внутреннего контроля



- Матрица требований НПА

По объектам контроля
По типам систем

- Опросные листы аудитора ИБ

По объектам контроля
По типам систем

- Шаблоны безопасности

Настройки встроенных СрЗИ
Настройки наложенных СрЗИ

- Результаты внутреннего контроля

Акт внутренней проверки
Собранные данные

- Обучение персонала

Курсы по СрЗИ
Повышение осведомленности

- Тестирование персонала

База вопросов
Индивидуальные тесты

- Сводная информация

Паспорта объектов контроля

- Аналитика

Срезы по состоянию безопасности организации
Дашборды

26. Итоги



Глубокий анализ требований НПА



Структурирование большого объема данных



Типизация критериев реализации



Типизация критериев контроля



Автоматизация рутинных задач



Централизованная унификация





ussc.ru



uralsecurity



Анастасия Федоренко

Руководитель направления «Автоматизация ИБ»
Аналитического центра УЦСБ

afedorenko@ussc.ru

+7 (932) 606-46-66

tg: Fedorenko_Anastasiia