

Практика идентификации и управления
изменениями элементов критичной
архитектуры **для финансовых организаций**



Александр Моисеев

Ведущий консультант по информационной
безопасности АКТИВ.CONSULTING

Система НПА и НМД для обеспечения ОН



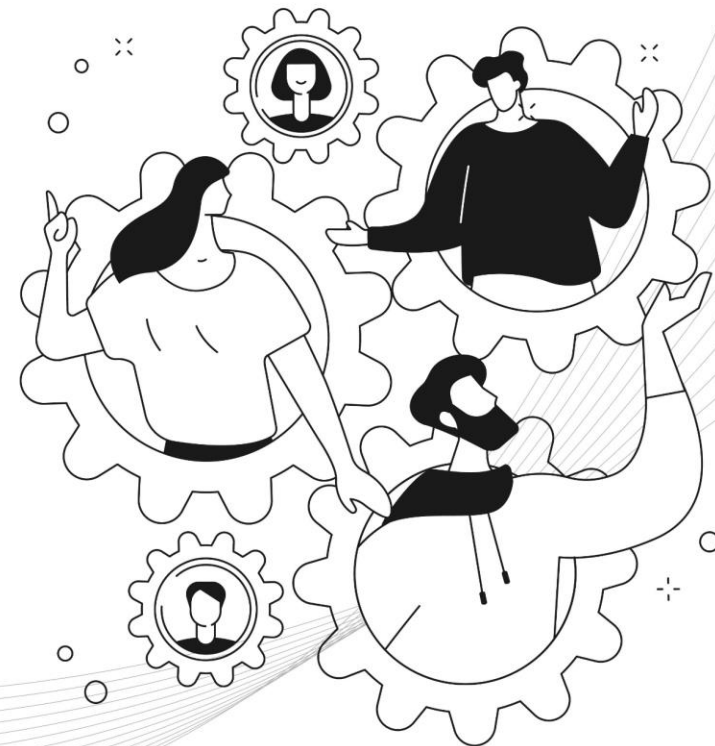
О чем сегодня пойдет речь

Процесс №1

Идентификация

Процесс №2

Управление
изменениями



Процесс №1 «Идентификация»



Выявление элементов КА

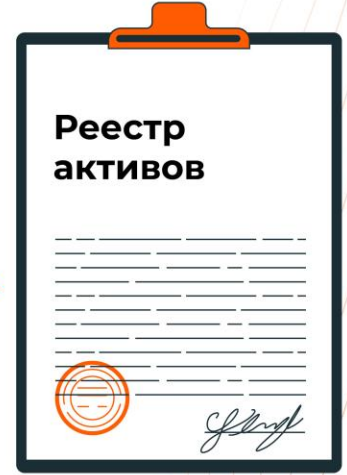
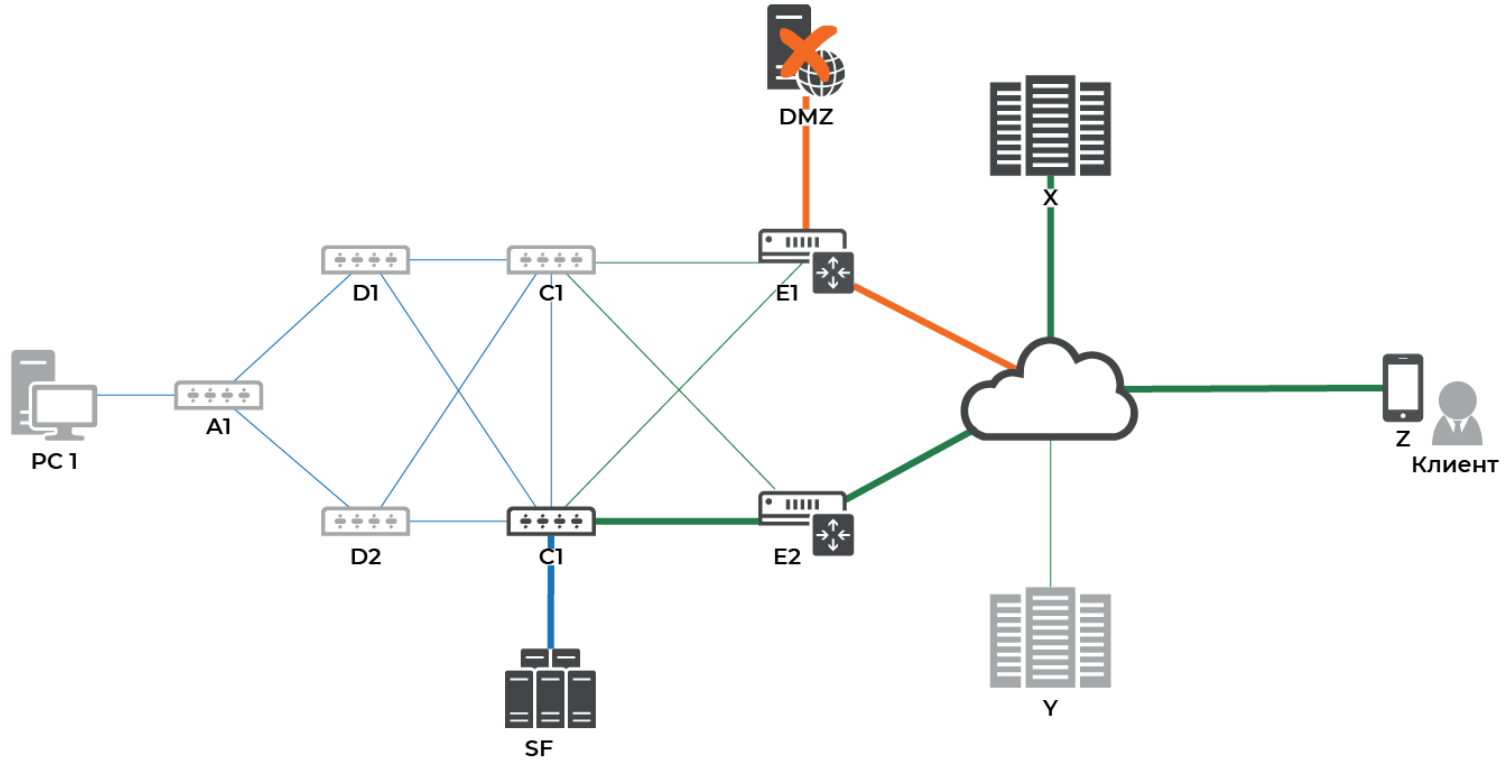


Классификация

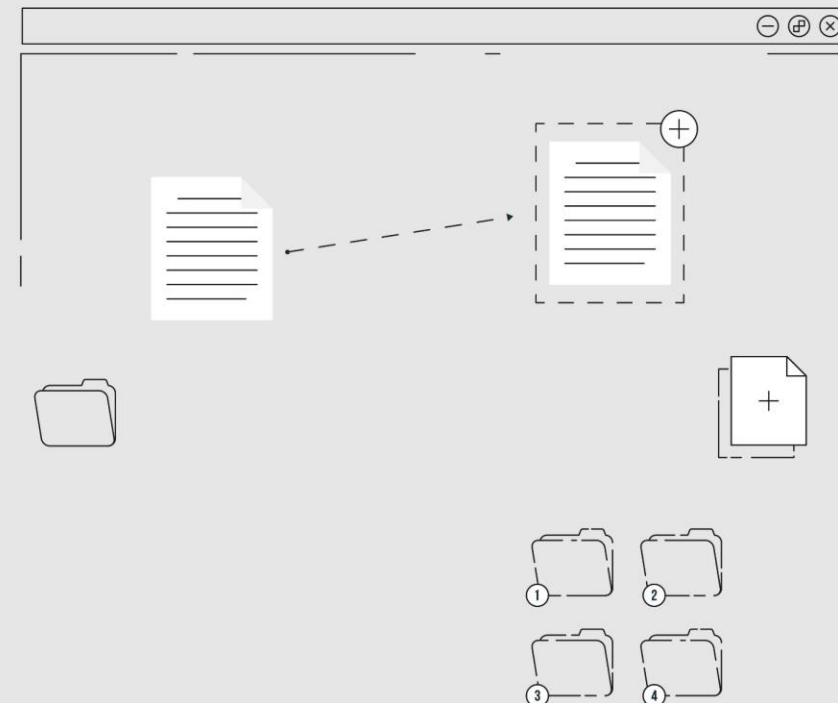


Учет элементов КА

Выявление элементов КА 1/3



Модель данных



Классификация 2/3

Пример классификации из СТО БР-1.5

Код ТУ	Наименование ТУ
[ИАА]	Идентификация, аутентификация и авторизация клиентов
[ФПП]	Формирование, передача и прием электронных сообщений
[УП]	Удостоверение права клиентов распоряжаться
[ОУ]	Осуществление финансовой операции
[ХИ]	Хранение информации

Пример реализации в ИС класса «SGRC»

The screenshot shows a software interface with a dark navigation sidebar on the left and a main content area on the right. The sidebar contains icons and labels for: ГЛАВНАЯ (Home), МОИ ДЕЛА (My Tasks), АКТИВЫ (Assets), РИСКИ (Risks), ТРЕБОВАНИЯ (Requirements), ЗАЩИТНЫЕ МЕРЫ (Protective Measures), and ТЕХНИЧЕСКИЕ УСЛОВИЯ (Technical Conditions). The main area displays a hierarchical list of processes:

- Linked | Процесс (Process)
- Linked | Операционный бизнес-процесс (Operational Business Process) - includes: Операционный бизнес процесс
- Team | Критически важный процесс (Critically Important Process) - includes: Критически важный процесс
- Team | Технологический процесс (Technological Process) - includes: Технологический процесс, ТП, Тех.процесс
- Team | Технологический участок (Technological Section) - includes: Технологический участок, ТУ
- Team | Идентификация, аутентификация и авторизация клиентов (ИАА)
- Team | Формирование электронных сообщений (ФПП)
- Team | Удостоверение права клиентов (УП)
- Team | Осуществление и учет финансовых операций (ОУ)
- Team | Хранение электронных сообщений (ХИ)

Учет элементов КА 3 / 3

Пример реализации учета активов

ГЛАВНАЯ

МОИ ДЕЛА

АКТИВЫ

РИСКИ

ТРЕБОВАНИЯ

ЗАЩИТНЫЕ МЕРЫ

ТЕХНИЧЕСКИЕ УЯЗВИМОСТИ

🔗 ХИ ТПрНФО16

Технологический участок , в нескольких местах расположения

Хранение электронных сообщений и информации об осуществленных финансовых операциях на торговой платформе (ХИ) в Технологическом процессе, обеспечивающим заключение договора между участниками организованный торгов (ТПрНФО16)

Содержание Показать граф связей

Актив не содержит других активов

Размещение (11)

↑	↑	↑
Postgre-as-a-service ↔ Системное ПО	Хранилище S3 ↔ Системное ПО	K8s-as-a-service ↔ Средство контейнеризации
↑	↑	↑
ЦОД 📍 Физическое пространство	ЦОД 📍 Физическое пространство	ЦОД 📍 Физическое пространство

Процесс №2 «Управление изменениями»



Управление изменениями



Управление конфигурацией ОИИ



Управление уязвимостями

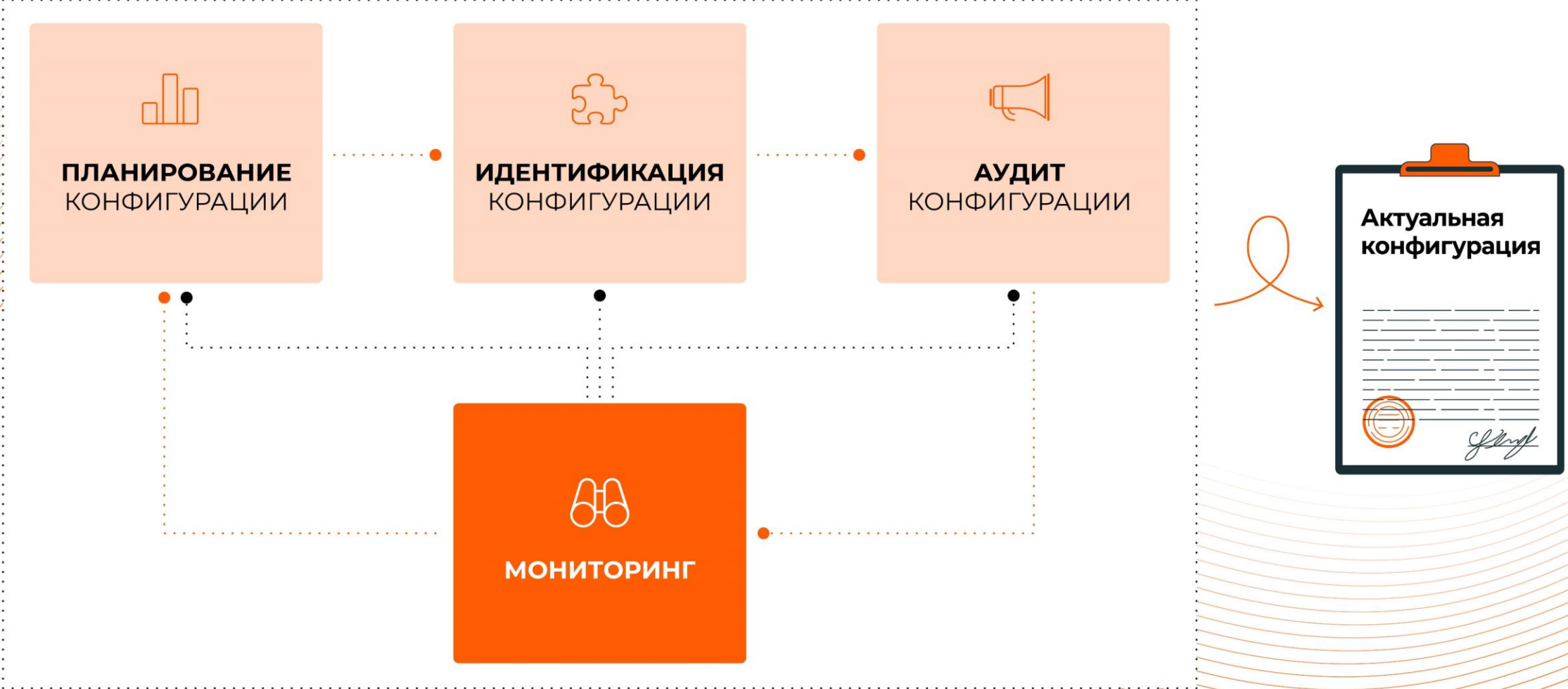


Управление обновлениями

Управление изменениями 1/4

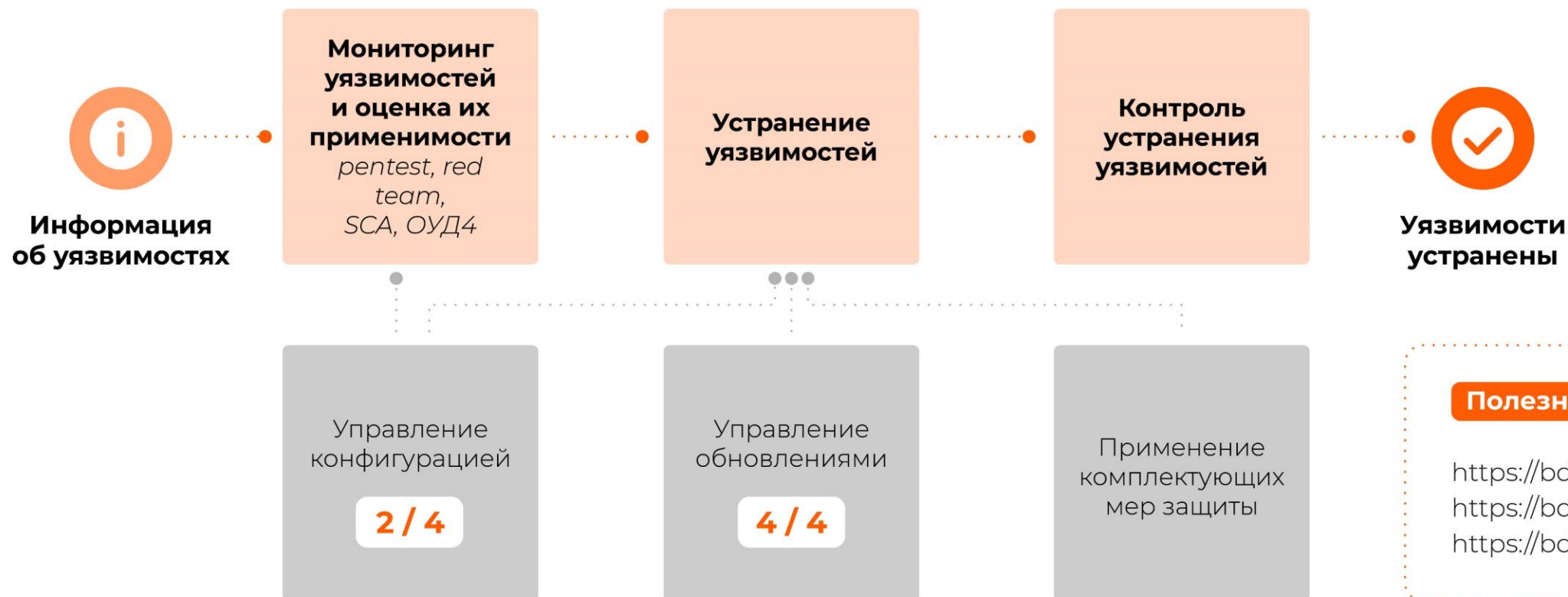


Управление конфигурацией 2 / 4



Управление уязвимостями 3 / 4

Пример схемы процесса управления уязвимостями





Полезные ссылки:

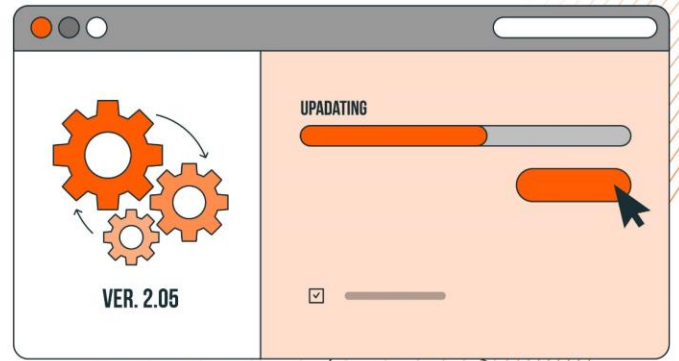
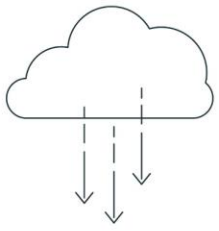
- <https://bdu.fstec.ru/vul>
- <https://bdu.fstec.ru/calc31>
- <https://bdu.fstec.ru/scanoval>

*Руководство по организации процесса управления уязвимостями (ФСТЭК России, 2023)







Управление обновлениями

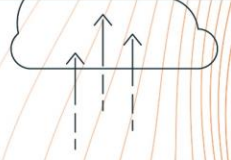
Тестирование обновлений

-  поиск актуальных обновлений
-  проверка корректности их работы



Тестирование безопасности обновлений

-  сверка идентичности (T001*)
-  проверка подлинности (T002)
-  антивирусный контроль (T003)
-  поиск опасных конструкций (T004)
-  мониторинг активности в среде функционирования (T005)
-  ручной анализ (T006)



Полезные ссылки:

<https://bdu.fstec.ru/software-section/updates>

*Методика тестирования обновлений безопасности ПО, ПАК (ФСТЭК России, 2022)

Выводы:

01

Разработка и адаптация методологии **под конкретное ФО**

02

Реализация процессов потребует **дополнительные ресурсы** для взаимодействия с ФинЦЕРТ

03

Цифровизация процессов сократит трудоемкость формирования отчетности для Банка России

04

Управление уязвимостями и обновлениями ПО с использованием **методологий ФСТЭК России**





Александр Моисеев

Ведущий консультант по информационной безопасности АКТИВ.CONSULTING

✉ moiseev@aktiv.consulting