Вебинар

psafe

От подходов к практике

безопасная разработка для АСУ ТП на примере разработки SCADA

ЧТО СЕГОДНЯ ОБСУДИМ

1. Приказ ФСТЭК 239: требования безопасной разработки
2. Как Apsafe помогает разработчикам SCADA
3. Особенности проектирования SCADA систем с учетом требований безопасной разработки
4. Сертификация – когда нужна?

Спикеры

Евгений Тодышев

МОДЕРАТОР

Руководитель направления безопасной разработки УЦСБ

Анастасия Камалова

СПИКЕР

Пресейл-инженер направления безопасной разработки УЦСБ

Виктор Тимашков

СПИКЕР

AppSec-аналитик группы инновационных решений направления безопасной разработки УЦСБ

Алла Очеретяная

СПИКЕР

Заместитель руководителя направления безопасной разработки в УЦСБ

01

ТРЕБОВАНИЯ ФСТЭК ПРИ РАЗРАБОТКЕ ПО ДЛЯ ЗОКИИ

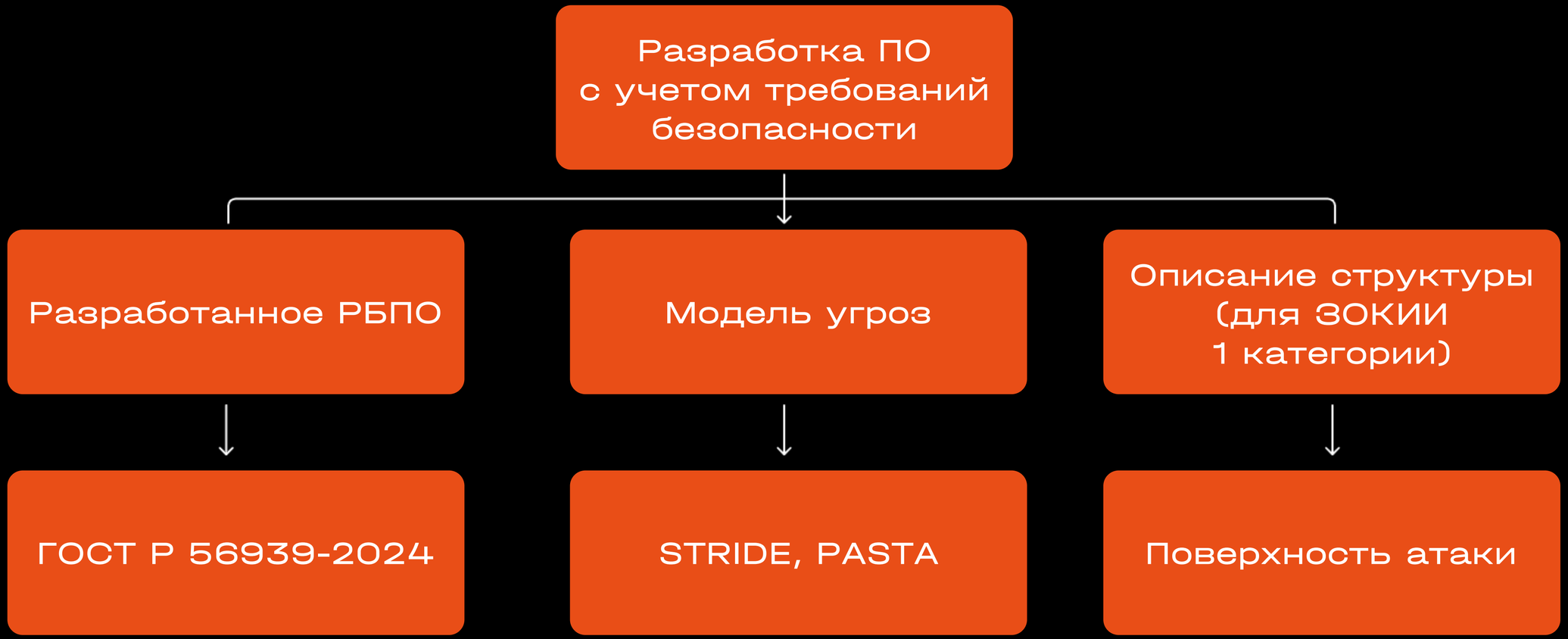
239 ПРИКАЗ ФСТЭК, П 29.3

Разработка ПО с учетом требований безопасности

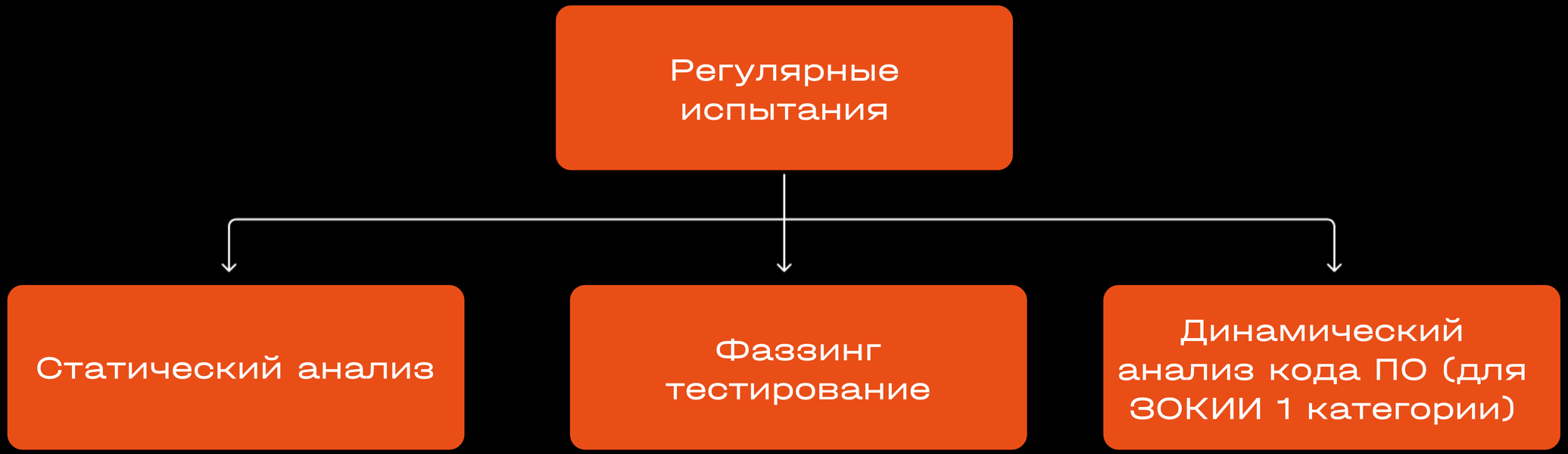
Проводить регулярные испытания

Поддержка безопасности ПО

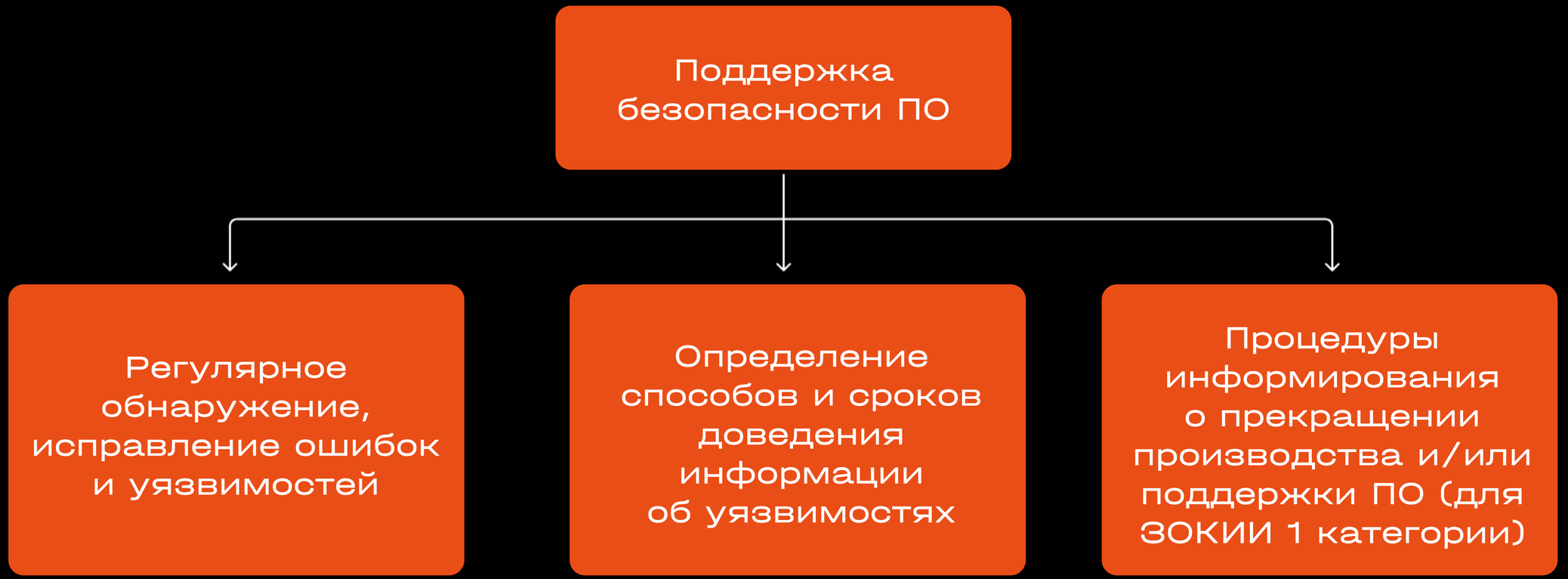
239 приказ ФСТЭК, п 29.3



239 приказ ФСТЭК, п 29.3



239 приказ ФСТЭК, п 29.3



02

КАК APSAFE ПОМОГАЕТ РАЗРАБОТЧИКАМ SCADA

Как Apsafe помогает разработчикам SCADA

- Формирование отчётов под Приказ ФСТЭК №239, ГОСТ 56939, PCI DSS v4, Приказ ФСТЭК №117 (будет в силе с 01.03.2026)
- Передаем аудиторам описание нашей платформы для подтверждения соответствия

Базовые стандарты безопасной разработки

Что применять всем, как best practice

СТАНДАРТ		ЧТО ДЕЛАТЬ?
ГОСТ Р 56939-2024	1	Внедрить статический и динамический анализ, SCA, проверку supply chain. Всё — как часть процесса разработки
ГОСТ Р 71207-2024	2	Использовать сертифицированный статический анализатор с нормальной точностью, API-интеграцией, фильтрацией ложных срабатываний
ГОСТ Р 58412-2019	3	Выявлять угрозы безопасности на всех этапах SDLC. Защищать сами процессы разработки
ГОСТ Р ISO/IEC 27034 (серия)	4	Построить secure SDLC: определить уровни доверия и применять меры ASC
ГОСТ Р 59793-2021	5	Обязательное прохождение стадий создания АС. Безопасность должна быть включена в ТЗ и проектирование
ГОСТ Р 57580.2-2018	6	Зрелость процессов разработки с ИБ ≥ уровень 4. Периодический аудит и повышение зрелости

Обязательные стандарты для соответствия

1: Операторы перс. данных **2: Субъекты КИИ** **3: Гос. ИС**

СТАНДАРТ		ЧТО ДЕЛАТЬ?
ФЗ-152 + Приказ ФСТЭК №21	1	Анализ кода на НДВ, пентесты, защищённое программирование — при высокой угрозе (1–2 тип)
ФСТЭК 239 (КИИ)	2	Статический анализ, фаззинг, динамический анализ (1-я категория), устранение уязвимостей, информирование пользователей
ФСТЭК 117 (ГИС)	3	Соблюдение ГОСТ 56939, контроль разработки (включая подрядчиков), регулярное сканирование кода, устранение уязвимостей

Отраслевые стандарты для соответствия

1: Финансовые организации

2: Субъекты электроэнергетики

3: Системы управления АЭС

4: Работа с платежными картами

СТАНДАРТ		ЧТО ДЕЛАТЬ?
ГОСТ 57580.1-2017	1	Для ОУД-4: анализ кода, контроль уязвимостей, либо сертифицированное ПО
Минэнерго 1215	2	Обязательная система патч-менеджмента и оповещения об уязвимостях со стороны разработчиков
ГОСТ 60880 / IEC 62859 (АЭС)	3	Проверка на скрытые функции и «unsafe code», особенно в критичных подсистема
PCI DSS v4.0	4	SDLC с безопасными практиками: обучение, контроль среды, устранение топ-уязвимостей, обновления, защита веб-приложений (WAF/DAST)

КЕЙСЫ ИЗ ПРАКТИКИ

Специфика SCADA-разработчиков

- Используются в ЗОКИИ
- Нет ИБ-специалистов
- Законодательство
- Бизнес-преимущество при продажах продукта

Кейс
Атомик Софт

On-prem SCADA-платформа

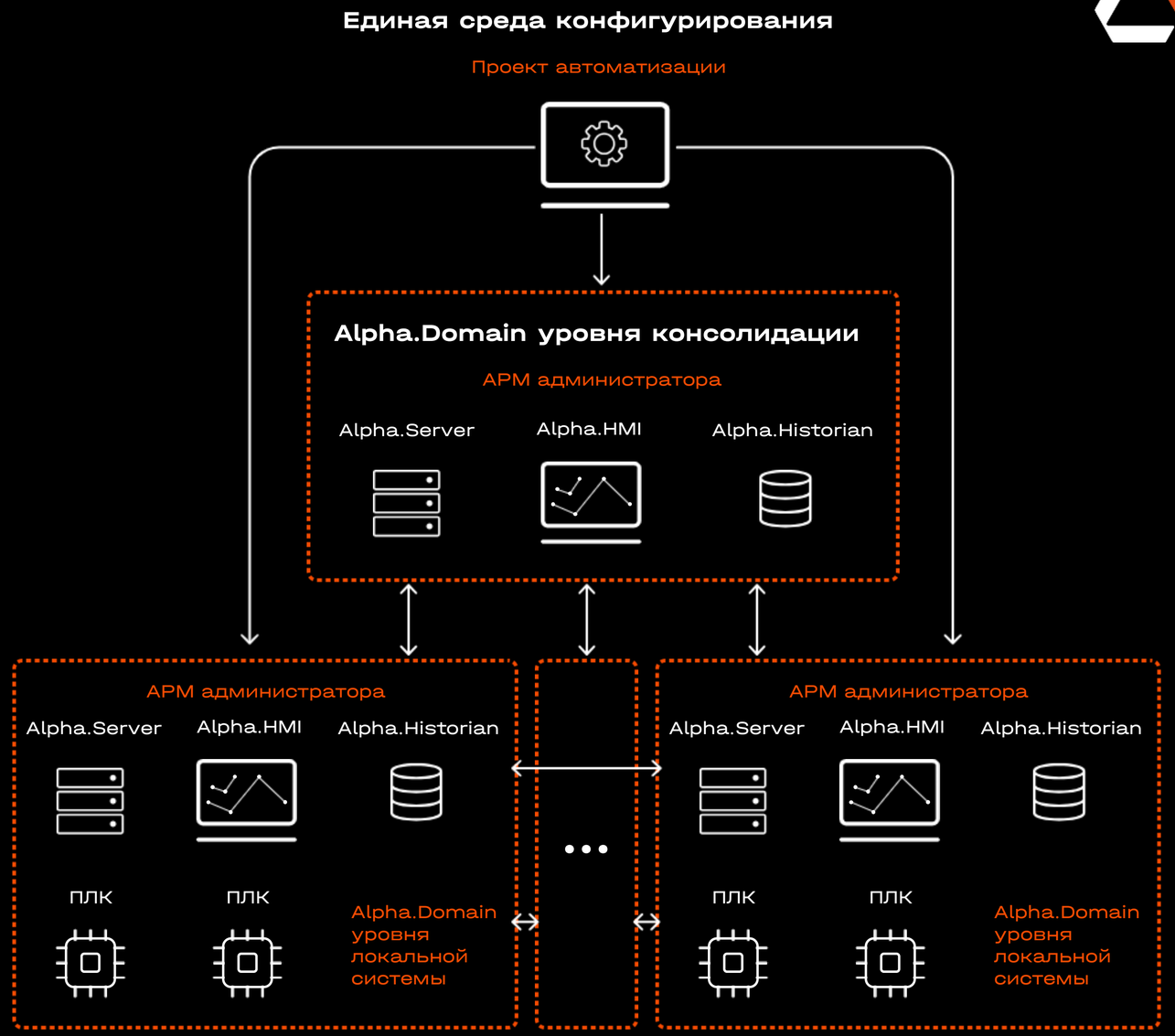
Коробочное решение

Состоит из 6 основных компонентов:

- Alpha.HMI
- Alpha.History
- Alpha.Security
- Alpha.Domain
- Alpha.Rmap
- Alpha.Server

Написаны с использованием C++

Каждый из модулей имеет собственный интерфейс для взаимодействия



Кейс
Атомик Софт

> Статический анализ кода:
> разработано порядка 100 правил

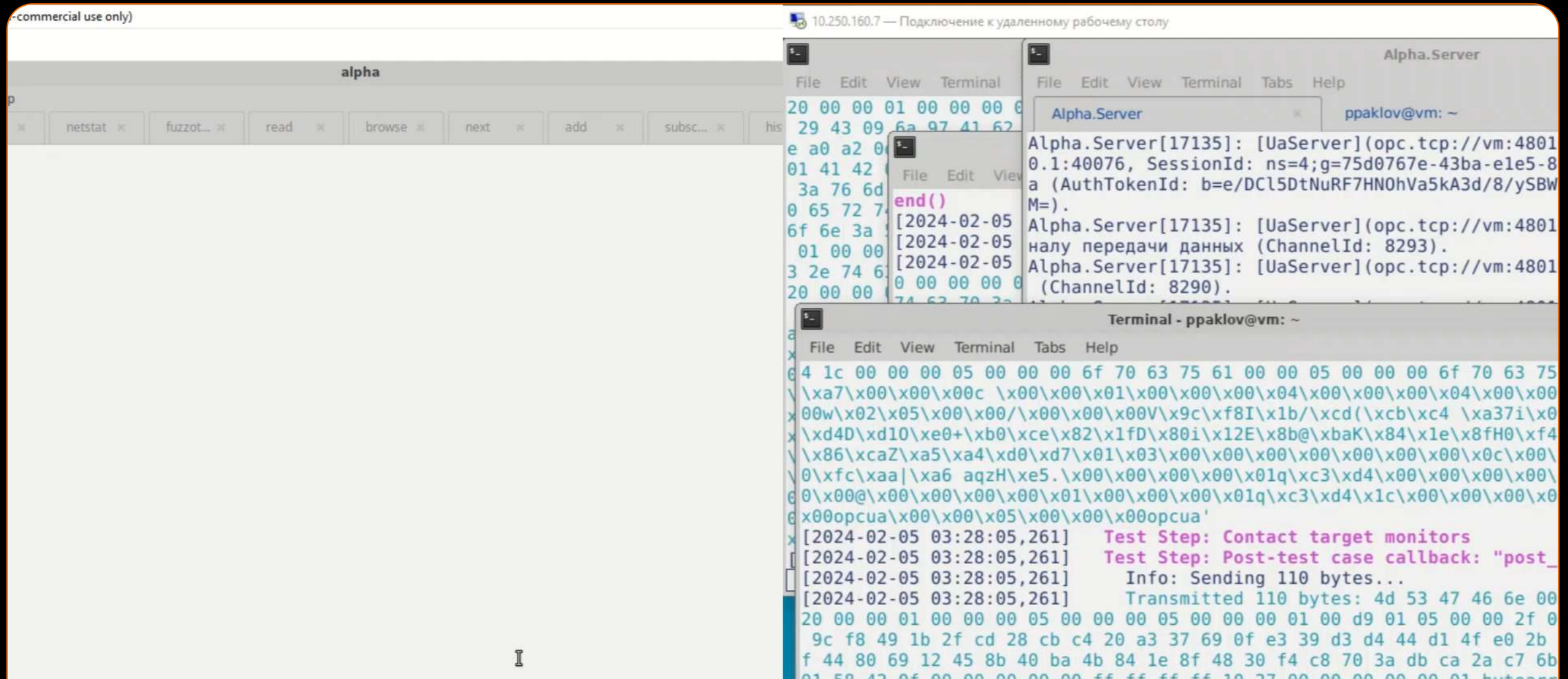
```yaml
rules:
  - id: Use-After-Free
    metadata:
      author: Victor 4ernyak <https://t.me/iter_malum>
      confidence: MEDIUM
      category: security
      cwe:
        - "CWE-416: Use After Free"
      vulnerability_class:
        - Memory Issues
    pattern-either:
    - patterns:
      - pattern: |
          free($PTR);
          ...
          $FUN(..., $PTR);
      - pattern-not: |
          free($PTR);
          ...
          $PTR = ...;
          ...
          $FUN(..., $PTR);
...
```

```yaml
rules:
  - id: NULL-Pointer-Dereference
    metadata:
      author: Victor 4ernyak <https://t.me/iter_malum>
      confidence: MEDIUM
      category: security
      cwe:
        - "CWE-476: NULL Pointer Dereference"
      vulnerability_class:
        - Memory Issues
    severity: HIGH
    pattern-either:
      - patterns:
          - pattern: |
              void $F(...,$STR *$PTR, ...)
              {
                ...
                $STR2 $VAR = $PTR->$STR3;
                ...
              }
...
```

Кейс

Атомик Софт

> Фаззинг-анализ: интерфейсов, протоколов, загрузки



Кейс

Атомик Софт

> Фаззинг-анализ: результат segmentation fault

```
[New Thread 0x7fffd14db640 (LWP 14180)]
414                                 PACKET d;
(gdb)
[New Thread 0x7fffd0cbd640 (LWP 14181)]
417                                 STL::deserializer des(pData, size);
(gdb)
[New Thread 0x7fffd048d640 (LWP 14183)]
418                                 des >> d.command >> d.transaction >> d.data;
(gdb)
[New Thread 0x7fffcfc65640 (LWP 14184)]
0x0000000000b19d5a in __gnu_cxx::__atomic_add_single (__val=<optimized out>, __mem=<optimized out>) at
 /opt/Automiq/gcc-5.5.0/include/c++/5.5.0/ext/atomicity.h:74
74      /opt/Automiq/gcc-5.5.0/include/c++/5.5.0/ext/atomicity.h: No such file or directory.
(gdb)
[New Thread 0x7fffcf43e640 (LWP 14185)]
tcp::CommandHandler::OnData (size=226, pData=<optimized out>, this=0x621000058d10) at /home/build/.con
an/data/Alpha.TcpTransport/5.6.7+b1.r101669/automiq/build/package/98ae183a3ee3f3e2bad76064b445e81aaaa2
a1b9/Interface/TcpTransport/helper/command_handler.h:420
420                             catch ( std::exception & )
(gdb)
[New Thread 0x7fffcec17640 (LWP 14186)]

Thread 43 "Alpha.Server" received signal SIGSEGV, Segmentation fault.
0x0000000000b00238 in STL::variant::clear (this=0x7fffd68f66c8) at /home/build/.conan/data/STL/1.2.6+b
1.r102102/automiq/build/package/5ab84d6acfe1f23c4fae0ab88f26e3a396351ac9/include/STL/STL/variant/varia
nt.hpp:96
96                                      m_placeholder->sub_ref();
```

Кейс
Атомик Софт

> Формируем задачи на устранение

[Apsafe] Test 7

« Предыдущее | 16/19 | Следующее »

Статус:	Новая	**Дата начала:**	06.09.2024
Приоритет:	Нормальный	**Срок завершения:**	
Назначена:	-	**Готовность:**	0%
Версия:	09.2024	**Оценка временных затрат:**	
severity:	medium	**status:**	Active, Verified
line_number:	42	**comment:**	test vulnerability comment
location:	login_controller.cp		

Описание

Цитировать

Result message: description of test vulnerability.

Кейс
Атомик Софт

Результаты

- На регулярной основе мы проводим все необходимые виды анализа
- Информация об уязвимостях оперативно доводится до разработчиков
- Проводим необходимые митапы с разработчиками
- Выполняем документальное сопровождение

СибКом Цифра
кейс №1

- Провели все согласования и настроили доступы
- Интегрировали платформу безопасности приложения с Jira клиента — уязвимости сразу попадают в таск-трекер
- На старте выявили 4 уязвимости высокого уровня критичности
- За несколько месяцев регулярных проверок найдены десятки уязвимостей
- Консультируем разработчиков по вопросам безопасной разработки

03

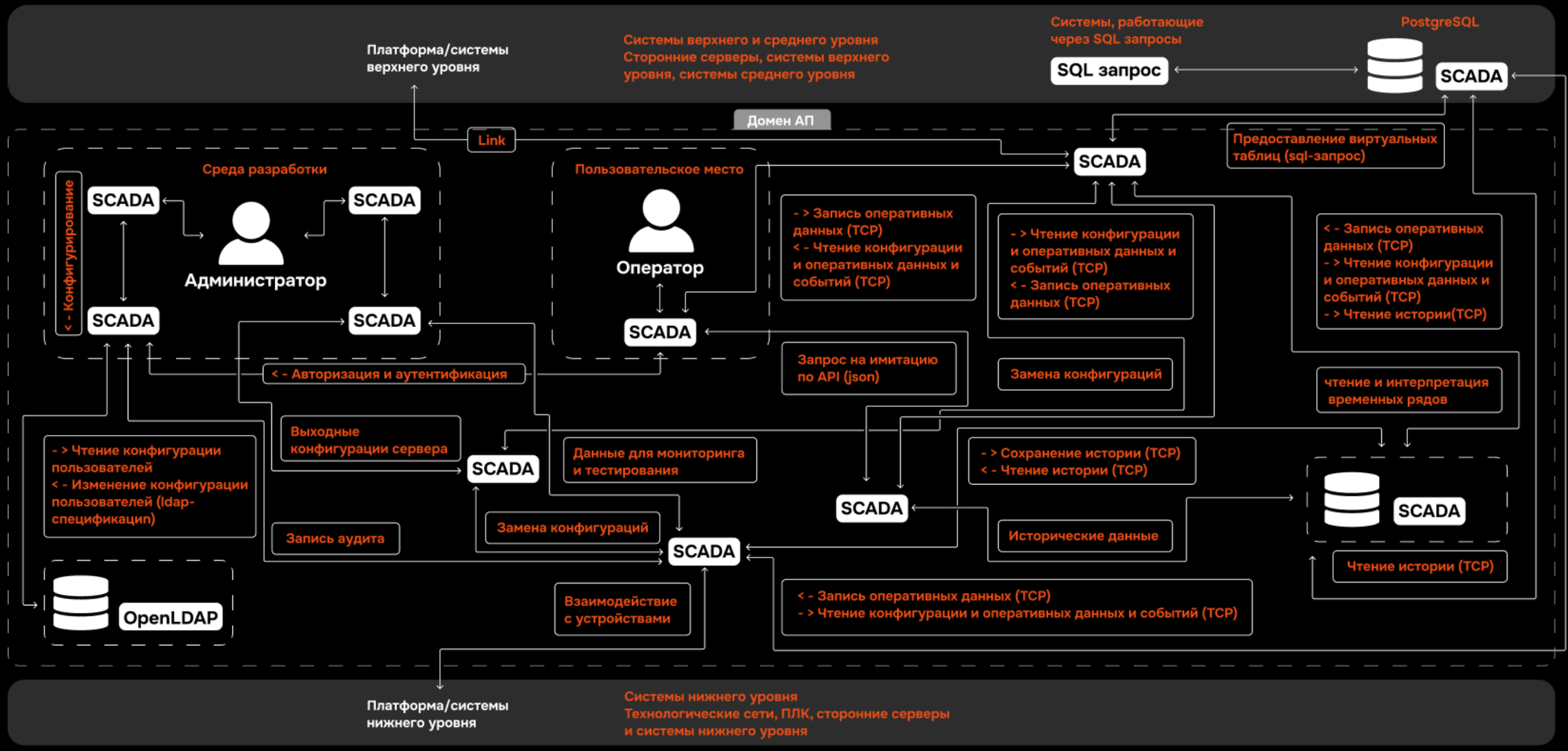
ОСОБЕННОСТИ ПРОЕКТИРОВАНИЯ SCADA СИСТЕМ С УЧЕТОМ ТРЕБОВАНИЙ БЕЗОПАСНОЙ РАЗРАБОТКИ

SCADA под прицелом

- 20% промышленных систем в России подверглись кибератакам*
- Источники угроз: интернет (вредоносные ресурсы, мессенджеры, облачные сервисы), почтовые клиенты, съемные носители
- Компрометация приводит к физическим последствиям: остановке производства, техногенным авариям, угрозе жизни людей

*по данным Kaspersky ICS CERT, 2025

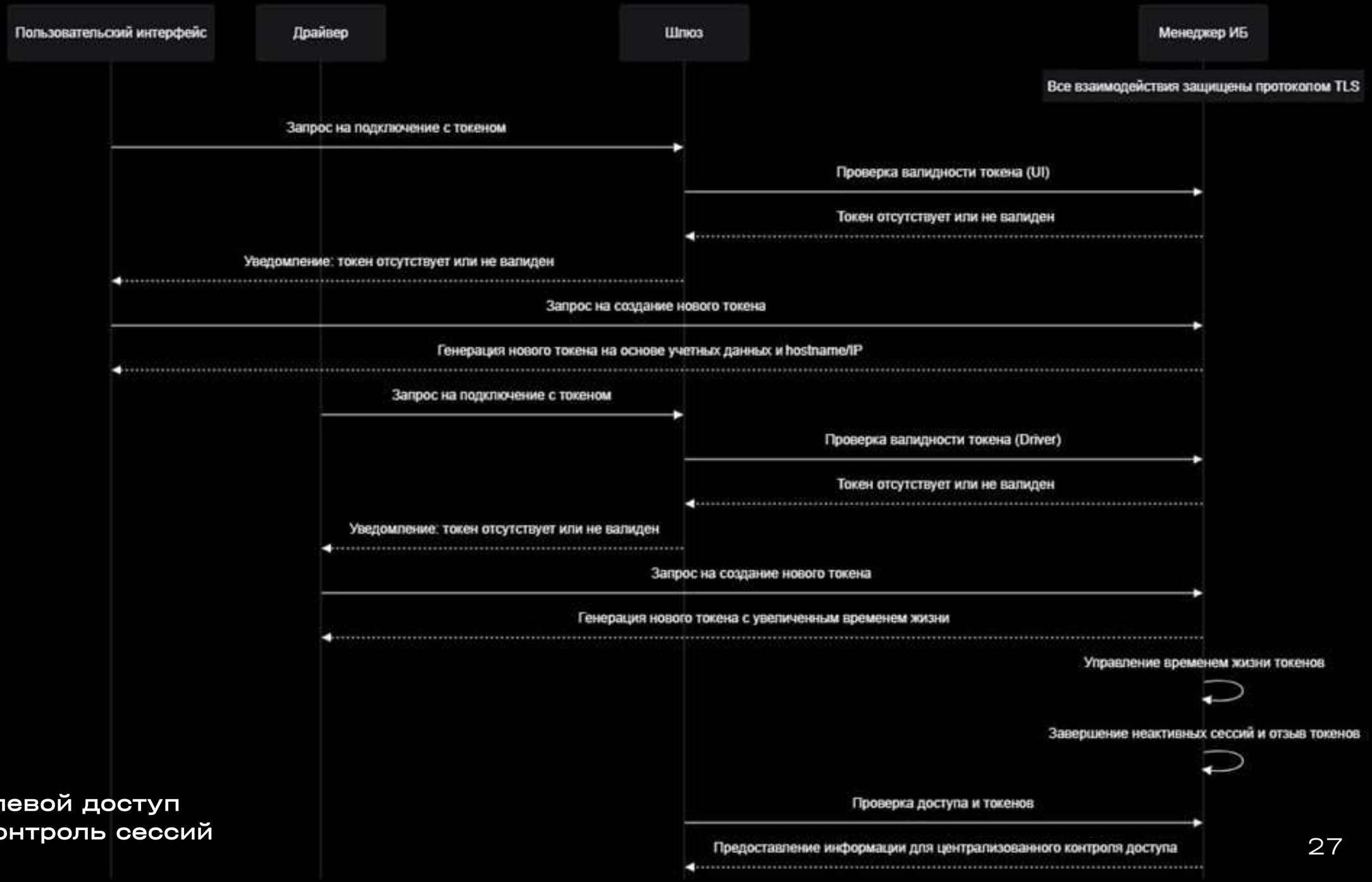
Каркас безопасности: требования стандартов



Главный вызов:
Ограничения промышленной среды

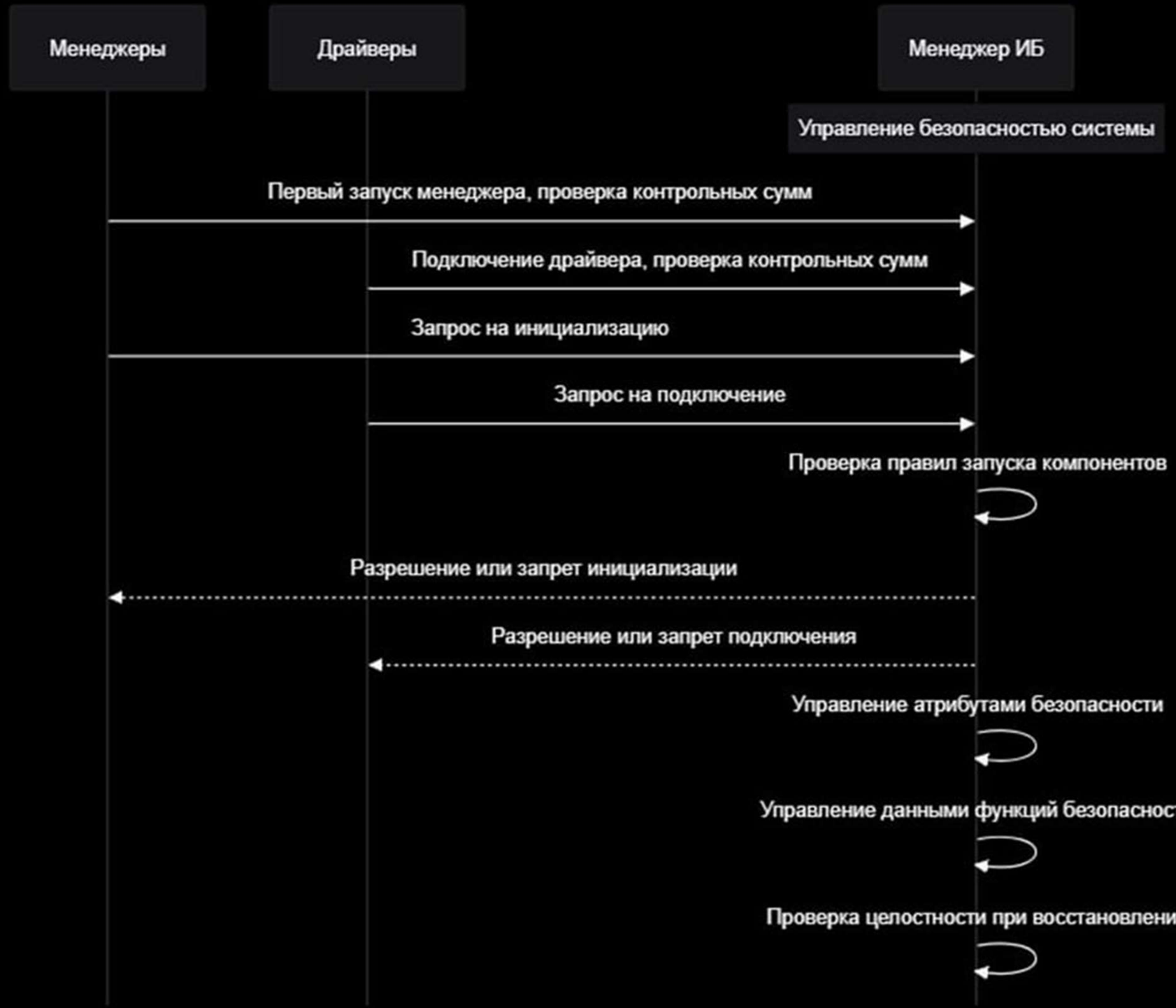
МЕРА БЕЗОПАСНОСТИ	ПРОБЛЕМА ПРИ РЕАЛИЗАЦИИ В SCADA
Ролевой доступ (RBAC) и контроль сессий	Интеграция с устаревшими HMI и промышленными протоколами, не поддерживающими сложные проверки доступа
Контроль целостности	Legacy ПЛК не поддерживают современные криптографические механизмы для цифровых подписей
Аудит и неизменяемость логов	Высокие требования к производительности и отсутствие поддержки централизованного логирования у legacy-устройств
Постоянная доступность	Высокая стоимость полного дублирования инфраструктуры для горячего резервирования
Уязвимости цепочек поставок	Необходимость оперативного применения обновлений без нарушения непрерывности процессов
Защита трафика	Несовместимость промышленных протоколов (Modbus, OPC) с современным шифрованием (TLS)
Многофакторная аутентификация	Отсутствие поддержки МФА в устаревшем оборудовании и HMI, усложнение оперативного доступа

Стандарт безопасности



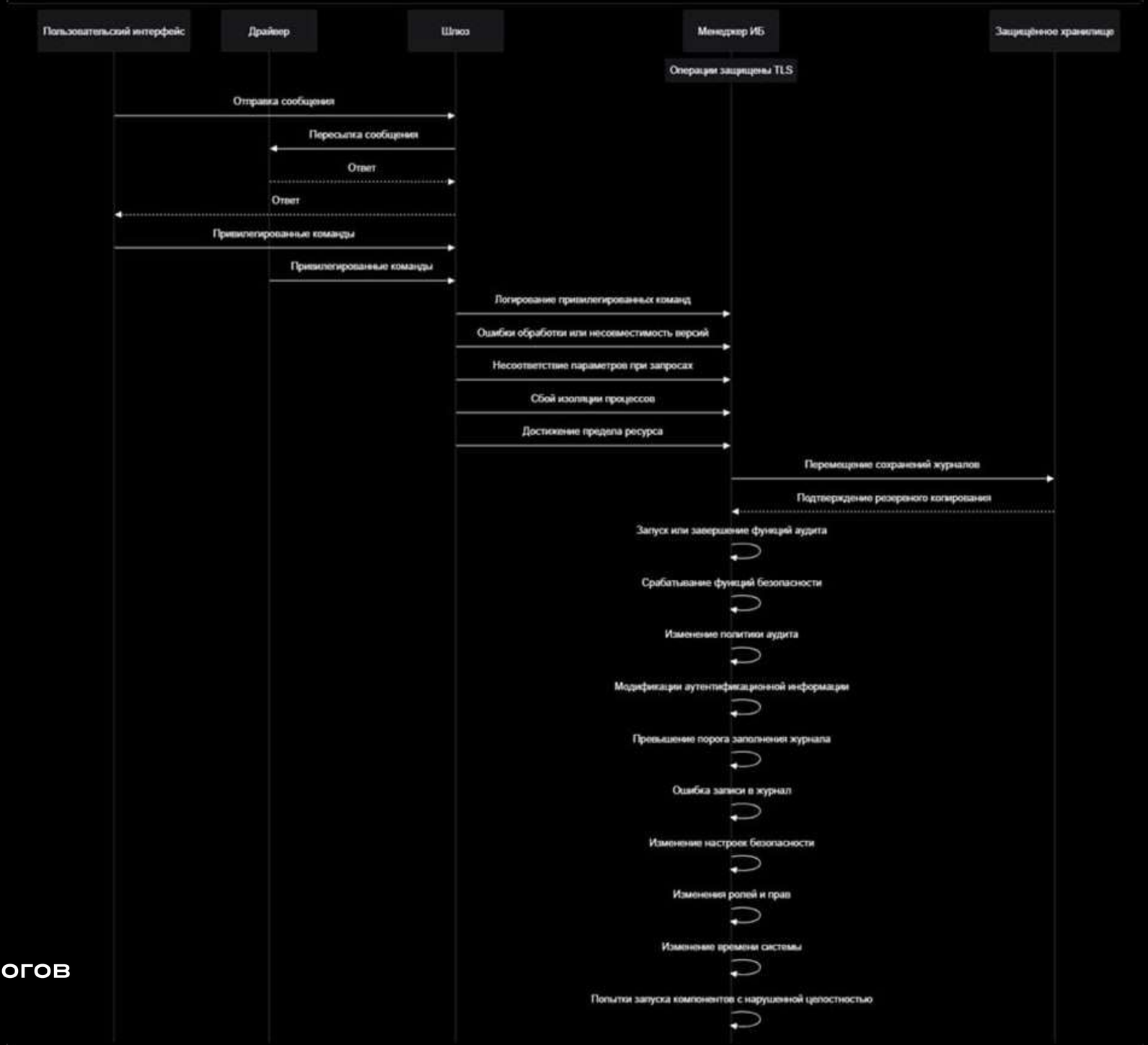
Мера 1: Ролевой доступ (RBAC) и контроль сессий

Стандарт безопасности



Мера 2: Контроль целостности

Стандарт безопасности



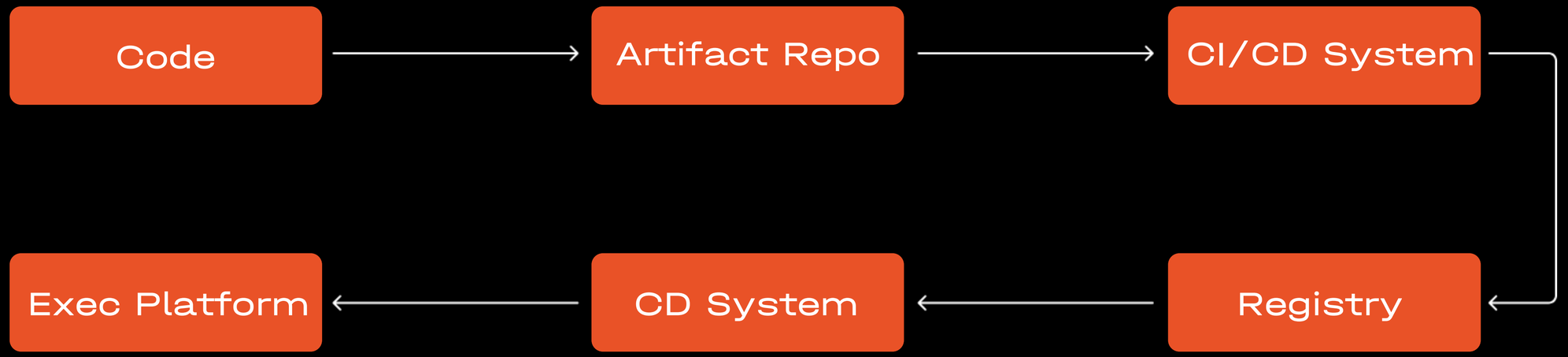
Мера 3: Аудит и неизменяемость логов

Стандарт безопасности

Мера 4: Постоянная доступность

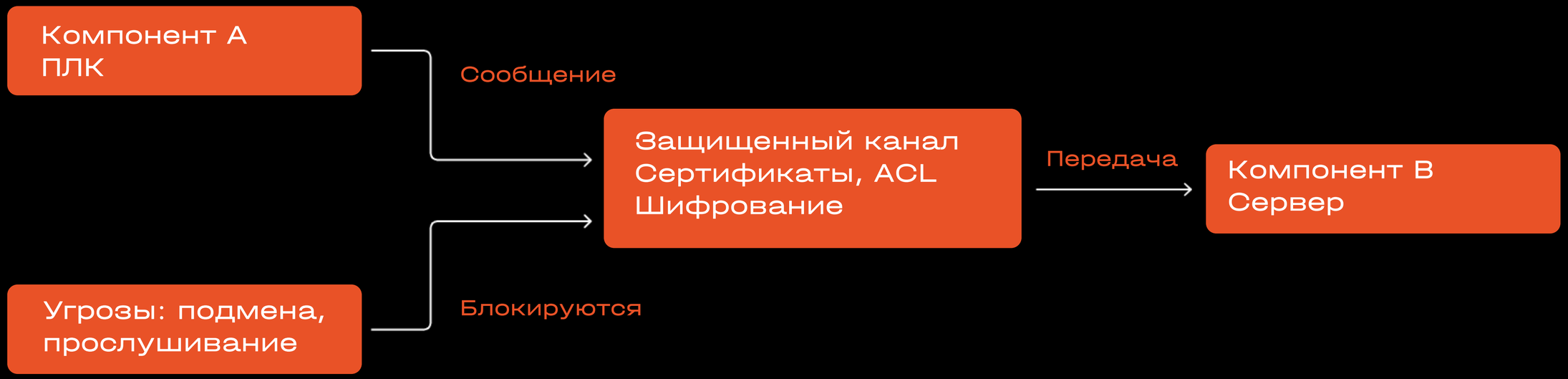
Стандарт безопасности

Мера 5: Уязвимости цепочек поставок



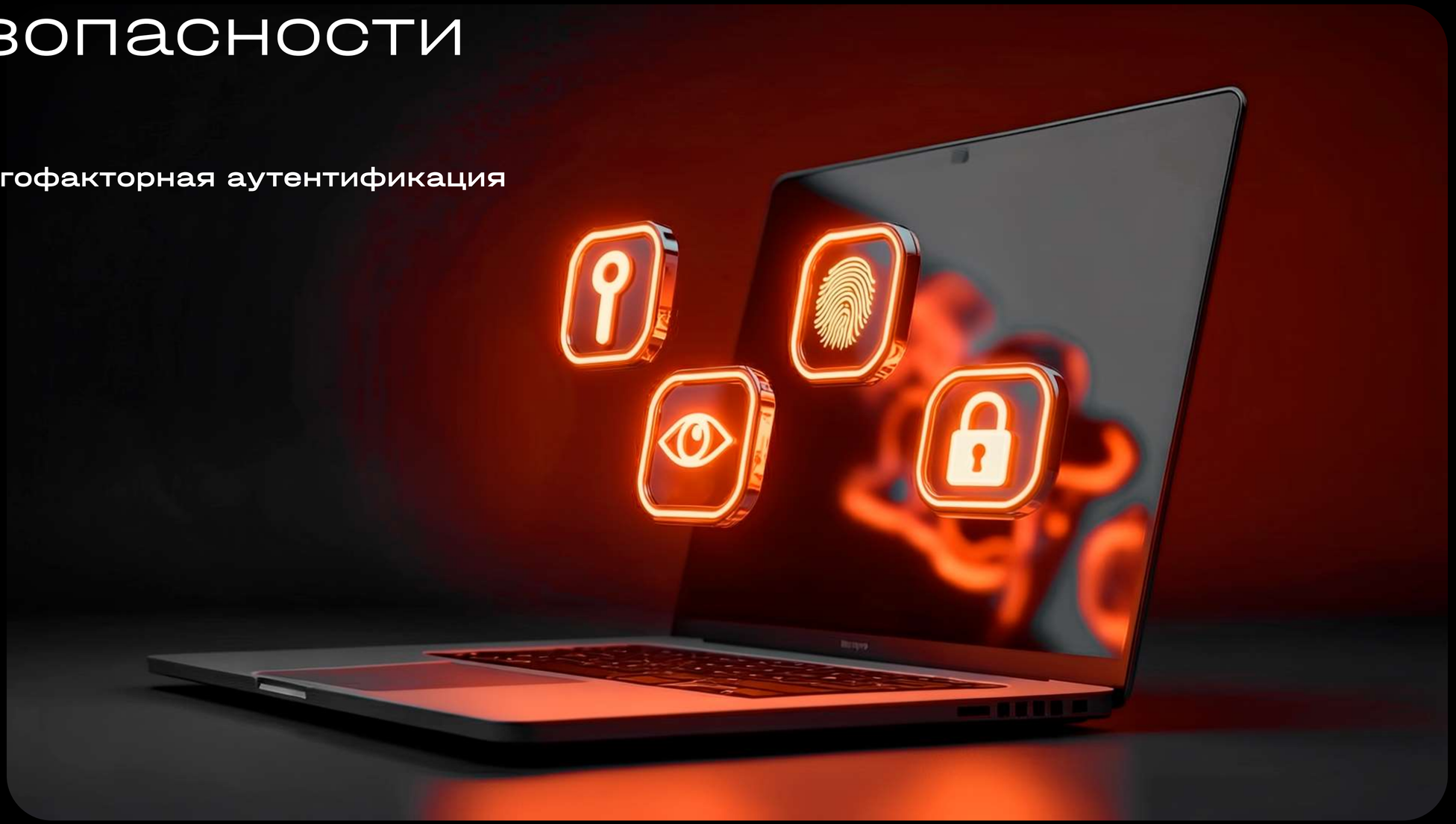
Стандарт безопасности

Мера 6: Защита трафика



Стандарт безопасности

Мера 7: Многофакторная аутентификация



04

СЕРТИФИКАЦИЯ – КОГДА НУЖНА?

Процесс сертификации

Приказ ФСТЭК России от 2 июня 2020 г. № 76

Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий

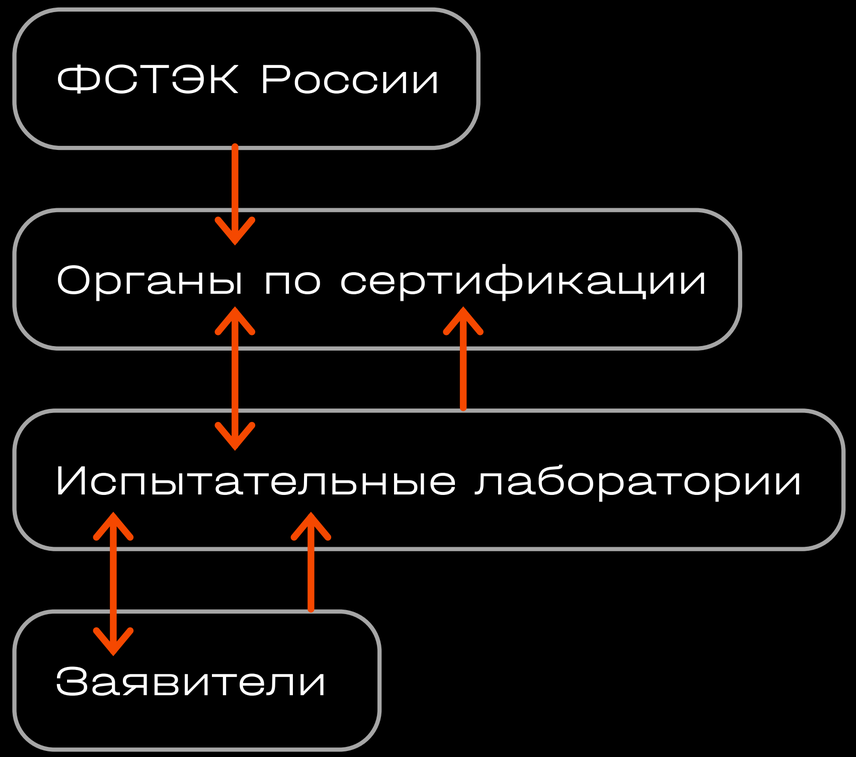
Приказ ФСТЭК России от 3 апреля 2018 г. № 55

Об утверждении положения о системе сертификации средств защиты информации

ГОСТ Р 56939-2024

Защита информации. Разработка безопасного программного обеспечения

Структура государственной системы сертификации СЗИ



Процесс сертификации

Этап 1

Заявка на сертификацию

Этап 2

Подготовка исходных данных

Этап 3

Договор на проведение сертификационных испытаний

Этап 4

Оформление результатов сертификационных испытаний

Этап 5

Оформление экспертного заключения по результатам сертификации

Этап 6

Выдача сертификата соответствия

Процесс сертификации

Этап 1

Заявка на сертификацию

Получение лицензий на деятельность по разработке СЗИ и лицензию на деятельность по технической защите конфиденциальной информации

Этап 2

Подготовка исходных данных

Этап 3

Договор на проведение сертификационных испытаний

Этап 4

Оформление результатов сертификационных испытаний

Этап 5

Оформление экспертного заключения по результатам сертификации

Этап 6

Выдача сертификата соответствия

Процесс сертификации

Соответствие между уровнем доверия и категорией КИИ и системами различных типов

УД СЗИ	КИИ	АСУ ТП
6	3	3
5	2	2
4	1	1
1, 2, 3	Государственная тайна	

Процесс сертификации

Этап 1

Заявка на сертификацию

Определить схему сертификации (единичный образец, партия, серия), необходимый уровень доверия

Этап 2

Подготовка исходных данных

Этап 3

Договор на проведение сертификационных испытаний

Этап 4

Оформление результатов сертификационных испытаний

Этап 5

Оформление экспертного заключения по результатам сертификации

Этап 6

Выдача сертификата соответствия

Процесс сертификации

Этап 1

Заявка на сертификацию

Этап 2

Подготовка исходных данных

Разработать минимальный комплект документов для подачи заявки

Этап 3

Договор на проведение сертификационных испытаний

Этап 4

Оформление результатов сертификационных испытаний

Этап 5

Оформление экспертного заключения по результатам сертификации

Этап 6

Выдача сертификата соответствия

Процесс сертификации

Приказ ФСТЭК России от 2 июня 2020 г. № 76
Для дифференциации требований по безопасности информации к средствам

Устанавливается 6 уровней доверия. Самый низкий уровень – шестой, самый высокий – первый

№ п/п	Наименование требования к уровню доверия	Уровень доверия		
		6	5	4
1.	Требования к разработке и производству средства:			
1.1.	требования к разработке модели безопасности средства			+
1.2.	требования к проектированию архитектуры безопасности средства	+	=	=
1.3.	требования к разработке функциональной спецификации средства	+	+	+
1.4.	требования к проектированию средства	+	=	=
1.5.	требования к разработке проектной (программной) документации	+	=	=
1.6.	требования к средствам разработки, применяемым для создания средства	+	=	=
1.7.	требования к управлению конфигурацией средства	+	+	+
1.8.	требования к разработке документации по безопасной разработке средства	+	=	+
1.9.	требования к разработке эксплуатационной документации	+	=	=
2.	Требования к проведению испытаний средства:			
2.1.	требования к тестированию средства	+	+	+
2.2.	требования к испытаниям по выявлению уязвимостей и недекларированных возможностей средства	+	+	+
2.3.	требования к проведению анализа скрытых каналов в средстве			+
3.	Требования к поддержке безопасности средства:			
3.1.	требования к устранению недостатков средства	+	+	+
3.2.	требования к обновлению средства	+	+	+
3.3.	требования к документированию процедур устранения недостатков и обновления средства	+	=	=
3.4.	требования к информированию об окончании производства и (или) поддержки безопасности средства	+	=	=

Процесс сертификации

Этап 1

Заявка на сертификацию

Этап 2

Подготовка исходных данных

Этап 3

Договор на проведение сертификационных испытаний

Выбрать испытательную лабораторию

Этап 4

Оформление результатов сертификационных испытаний

Этап 5

Оформление экспертного заключения по результатам сертификации

Этап 6

Выдача сертификата соответствия

Процесс сертификации

Этап 1

Заявка на сертификацию

Этап 2

Подготовка исходных данных

Этап 3

Договор на проведение сертификационных испытаний

Подача заявки на сертификацию

Этап 4

Оформление результатов сертификационных испытаний

Этап 5

Оформление экспертного заключения по результатам сертификации

Этап 6

Выдача сертификата соответствия

Процесс сертификации

Этап 1

Заявка на сертификацию

Этап 2

Подготовка исходных данных

Этап 3

Договор на проведение сертификационных испытаний

Этап 4

Оформление результатов сертификационных испытаний

Сертификационные испытания СЗИ

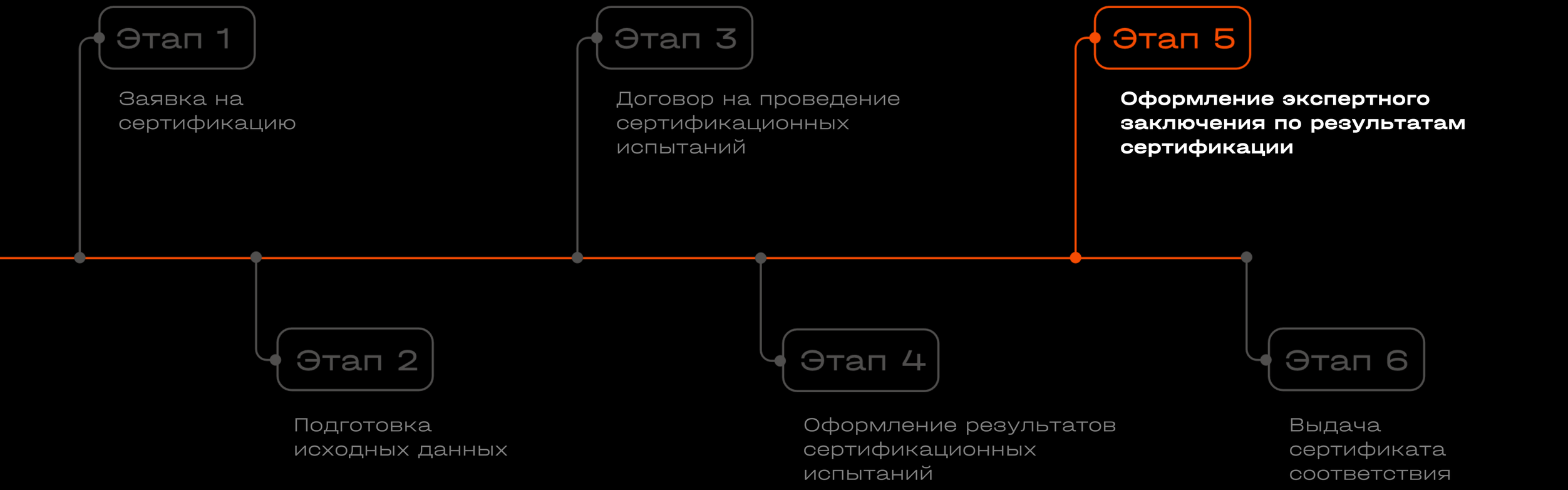
Этап 5

Оформление экспертного заключения по результатам сертификации

Этап 6

Выдача сертификата соответствия

Процесс сертификации



Процесс сертификации

Этап 1

Заявка на сертификацию

Этап 2

Подготовка исходных данных

Этап 3

Договор на проведение сертификационных испытаний

Этап 4

Оформление результатов сертификационных испытаний

Этап 5

Оформление экспертного заключения по результатам сертификации

Этап 6

Выдача сертификата соответствия

Безопасность под ключ

- Анализ выполнения требований безопасности
- Разработка модели угроз ПО
- Аудит и разработка рекомендаций по повышению уровня зрелости
- Ревью архитектуры и кода
- Управление уязвимостями в разработке
- Построение безопасной разработки как процесса
- Обучение разработчиков

200+
проектов в течение года

Экспертное консультирование и сопровождение в процессе сертификации

Выбор, пилотирование и внедрение инструментов OSA, SAST, DAST, OSA, SCA анализа

Apsafe - платформа для непрерывного анализа защищенности приложений

СПАСИБО!

Для участников вебинара:

- Бесплатный пилот Apsafe
- Дарим мерч за лучший вопрос

apsafe.ru