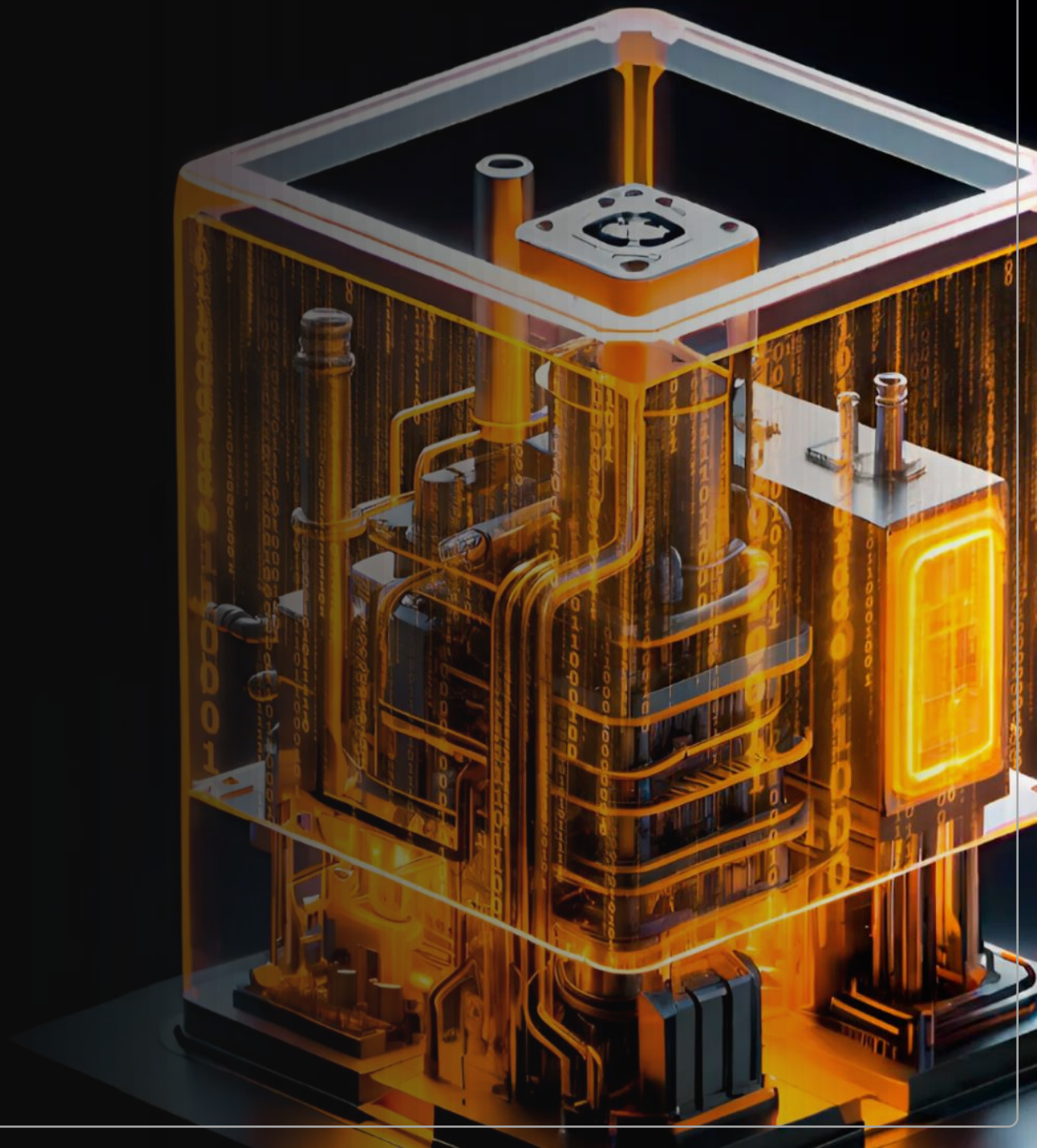




Безопасная разработка ПО для значимых объектов КИИ

VI вебинар цикла «Обеспечение безопасности объектов КИИ
в рамках 187-ФЗ»



ПЛАН ВЕБИНАРА

- 01** Актуальность внедрения БРПО
- 02** Элементы процесса безопасной разработки
- 03** Инструменты для реализации процессов безопасной разработки
- 04** Практические кейсы

АКТУАЛЬНОСТЬ

SUPPLY CHAIN

ДЕКАБРЬ 2020

несколько правительственных агентств США были взломаны через обновление ПО Orion, разработки SolarWinds

МАРТ 2022

в прт-модуль node-ipc внедрен вредоносный код, удаляющий данные с сервера

АВГУСТ 2022

выложен в открытый доступ исходный код продуктов Right Line

ОКТАБРЬ 2021

в прт-пакет UAParser.js внедрили вредоносный код, который похищал учетные данные

АВГУСТ 2022

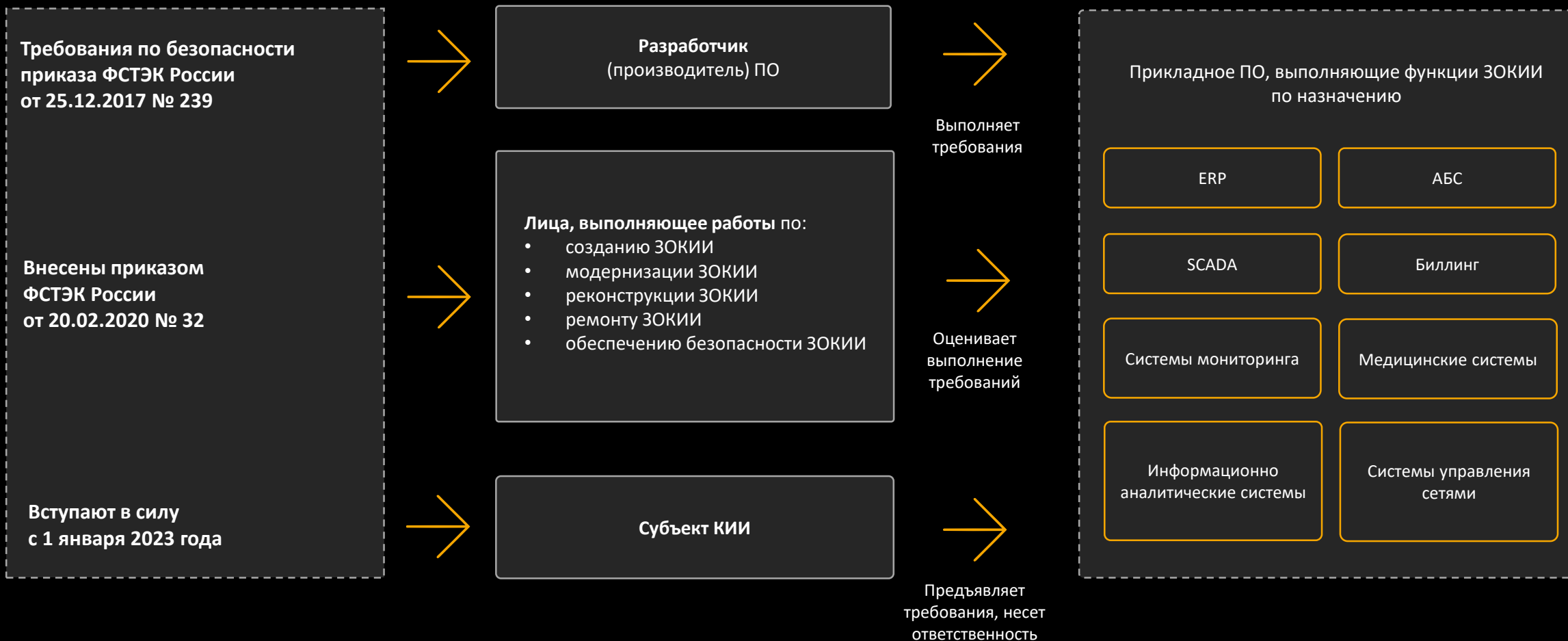
обнаружено несколько вредоносных пакетов в PyPI

ОПРОС №1

**Выполняете ли вы требования ФСТЭК
по безопасной разработке?**

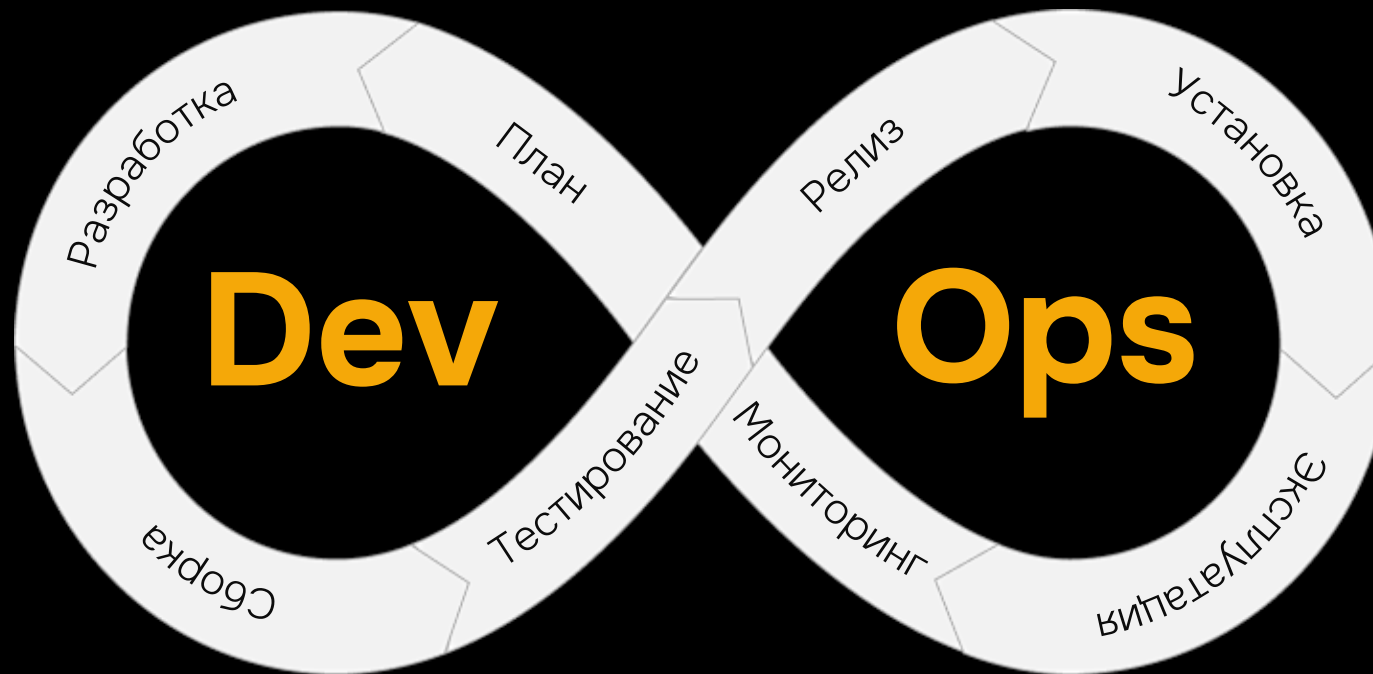
АКТУАЛЬНОСТЬ

П.29.3 ПРИКАЗА ФСТЭК РОССИИ №239



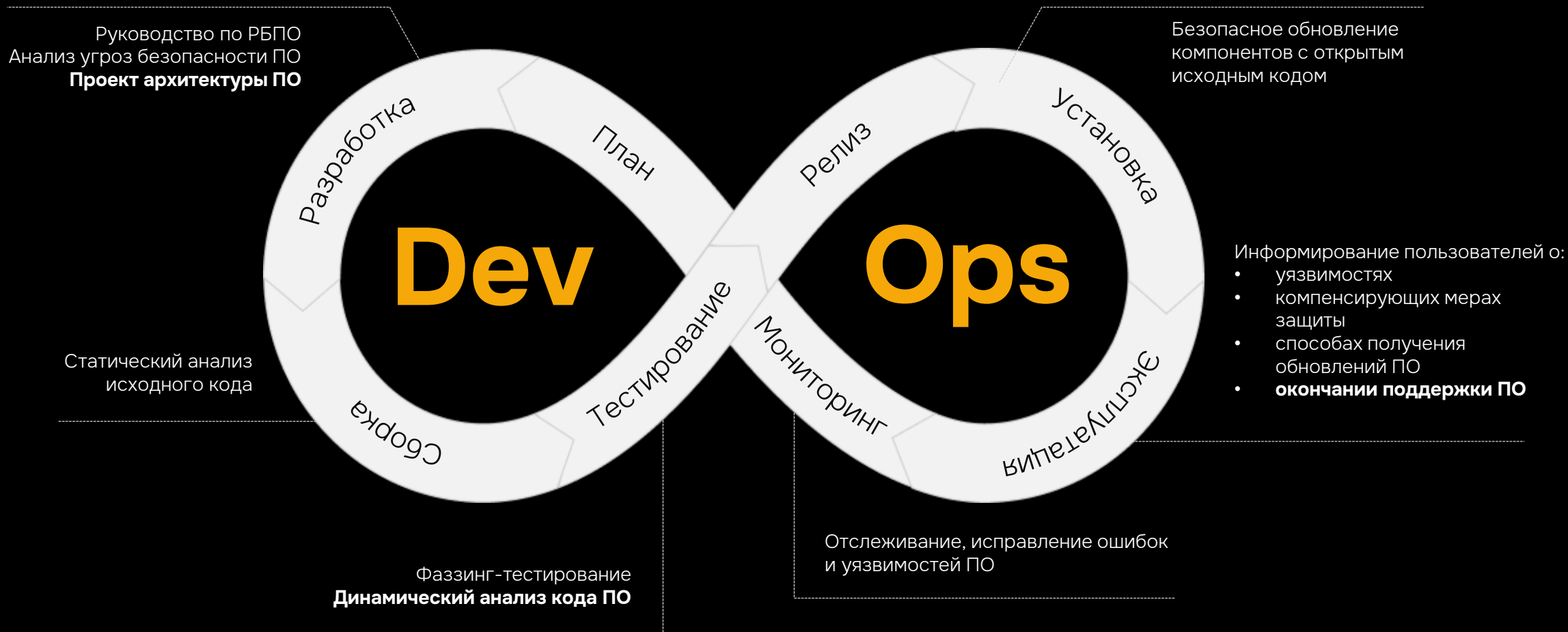
АКТУАЛЬНОСТЬ

П.29.3 ПРИКАЗА ФСТЭК РОССИИ №239



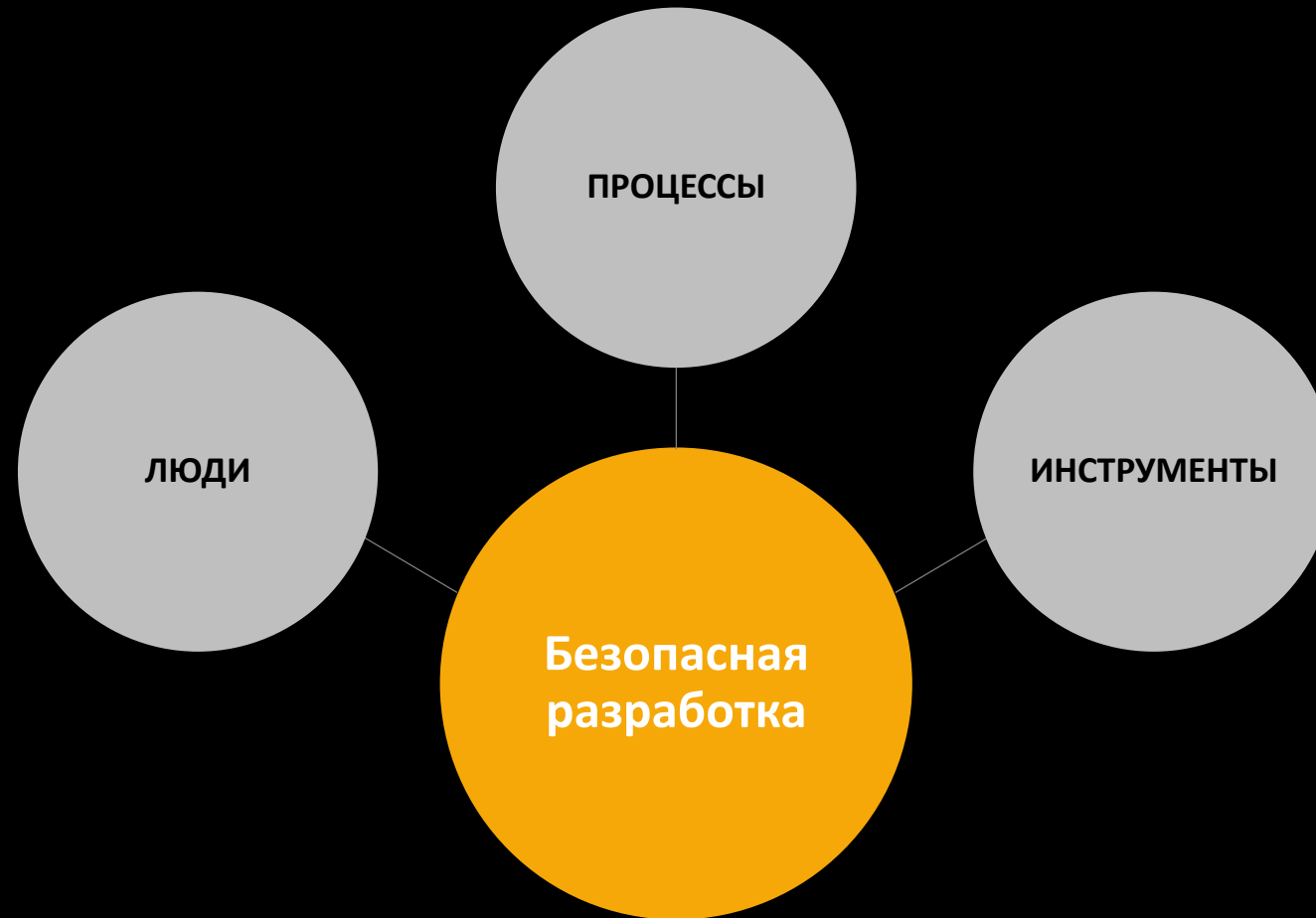
АКТУАЛЬНОСТЬ

П.29.3 ПРИКАЗА ФСТЭК РОССИИ №239



КАК ЭТО СДЕЛАТЬ?

ЭЛЕМЕНТЫ



КАК ЭТО СДЕЛАТЬ?

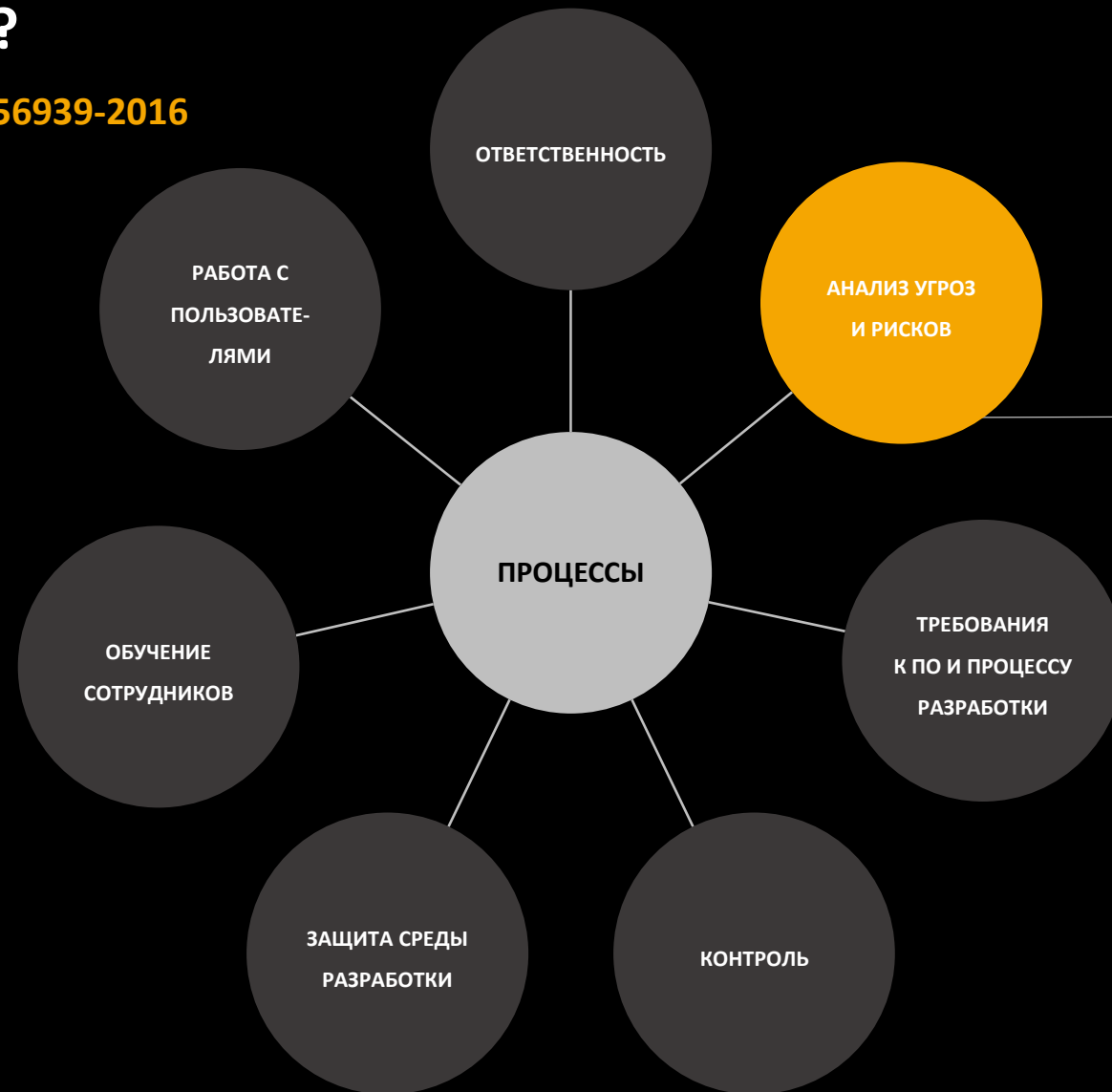
В СООТВЕТСТВИИ С ГОСТ Р 56939-2016

- ответственные за выполнение и контроль мер в процессе разработки
- анализ текущих процессов разработки
- взаимодействие с пользователями



КАК ЭТО СДЕЛАТЬ?

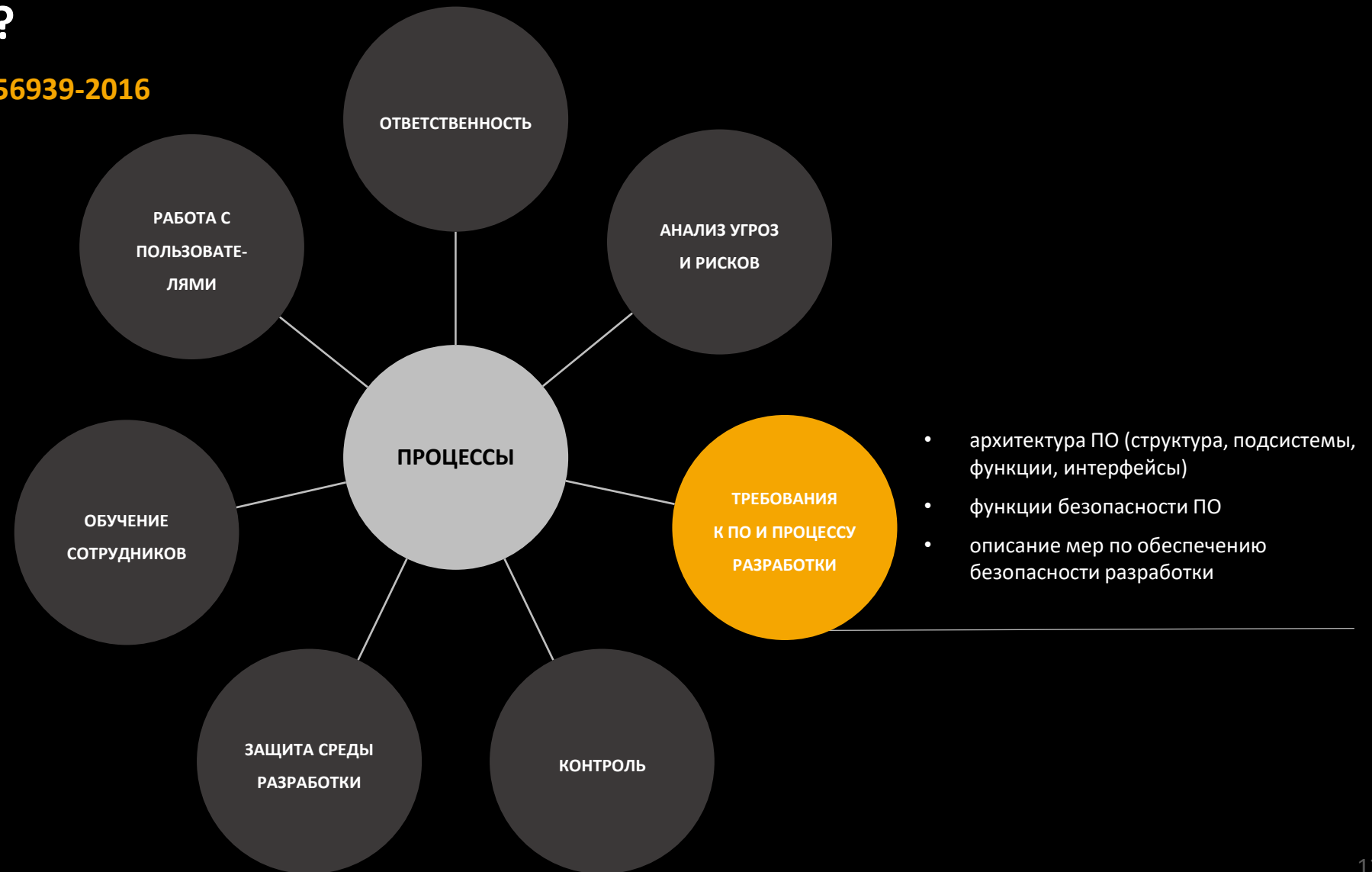
В СООТВЕТСТВИИ С ГОСТ Р 56939-2016



- угрозы безопасности
- риски в процессе разработки
- описание проектных решений или компенсирующих мер по минимизации рисков и предотвращению угроз

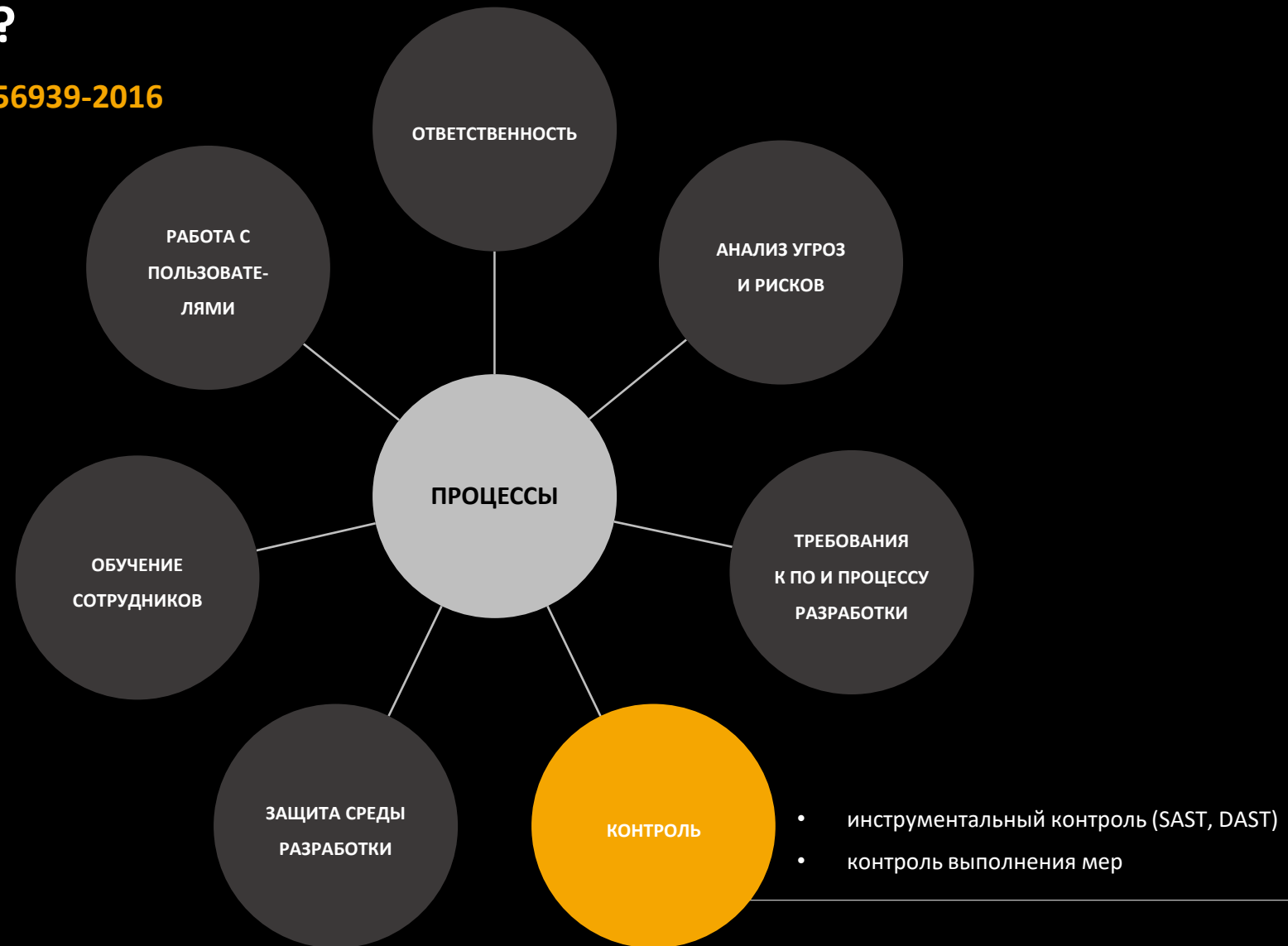
КАК ЭТО СДЕЛАТЬ?

В СООТВЕТСТВИИ С ГОСТ Р 56939-2016



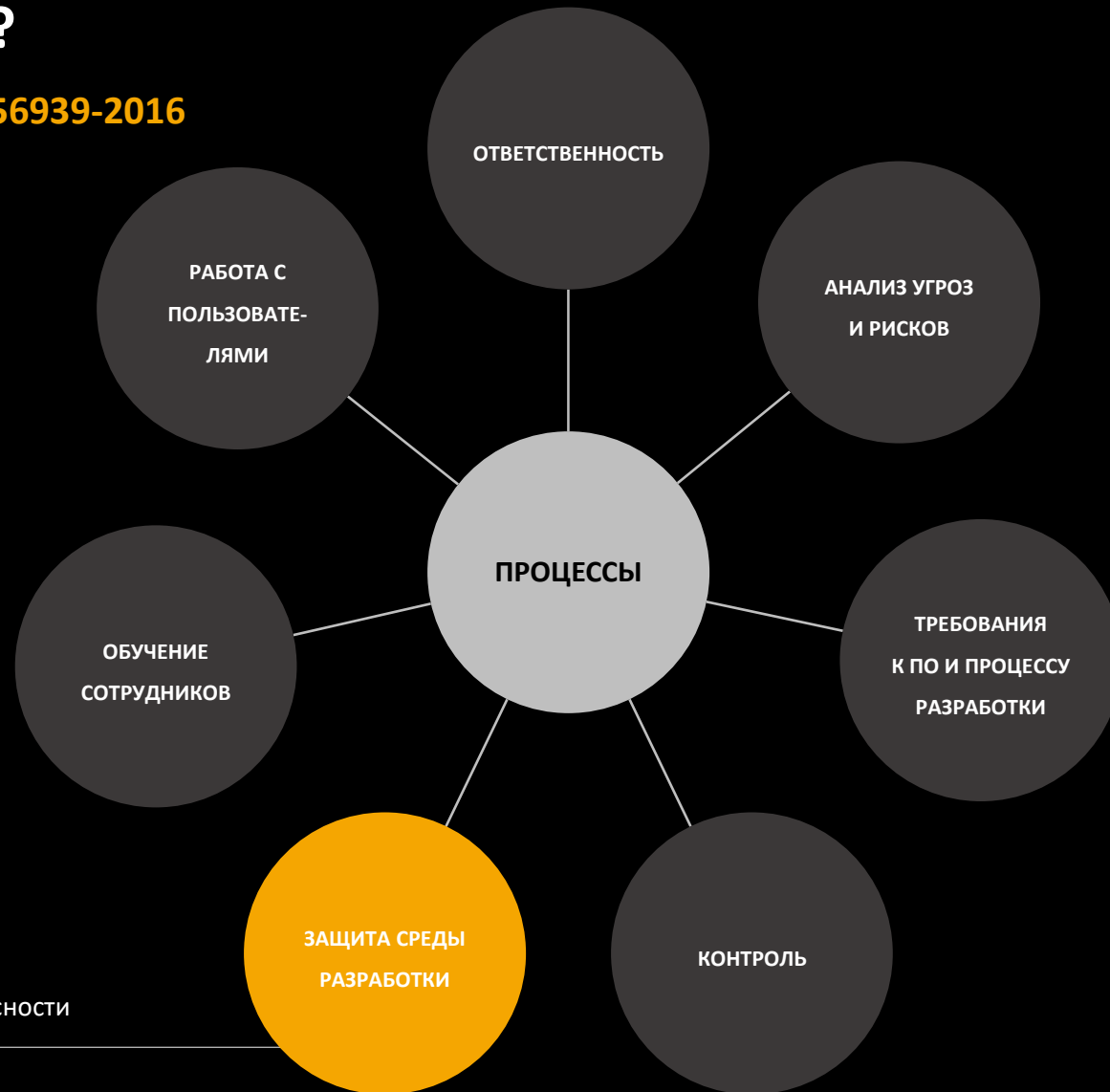
КАК ЭТО СДЕЛАТЬ?

В СООТВЕТСТВИИ С ГОСТ Р 56939-2016



КАК ЭТО СДЕЛАТЬ?

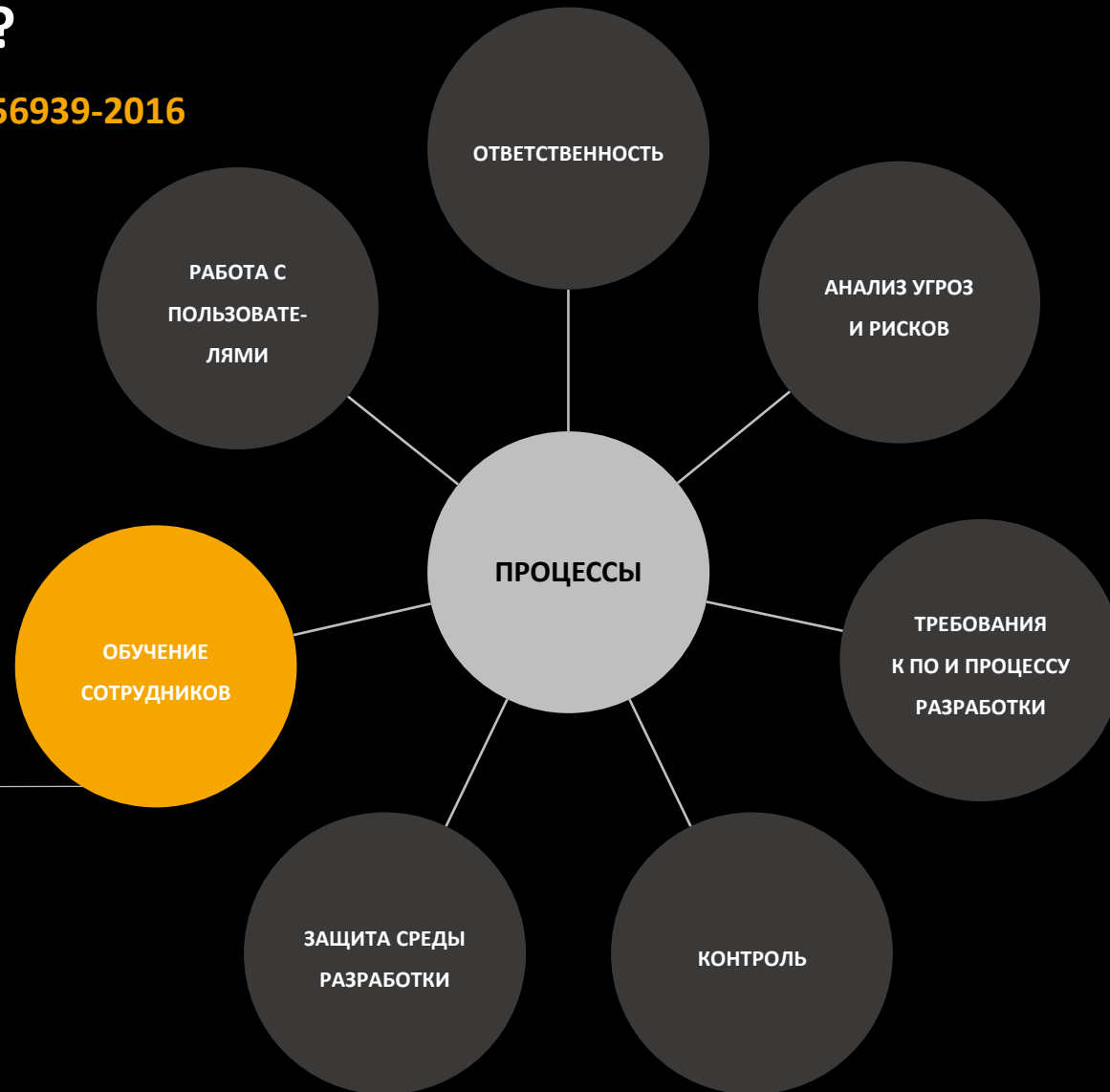
В СООТВЕТСТВИИ С ГОСТ Р 56939-2016



- защита от НСД среды разработки
- резервное копирование
- регистрация событий безопасности

КАК ЭТО СДЕЛАТЬ?

В СООТВЕТСТВИИ С ГОСТ Р 56939-2016

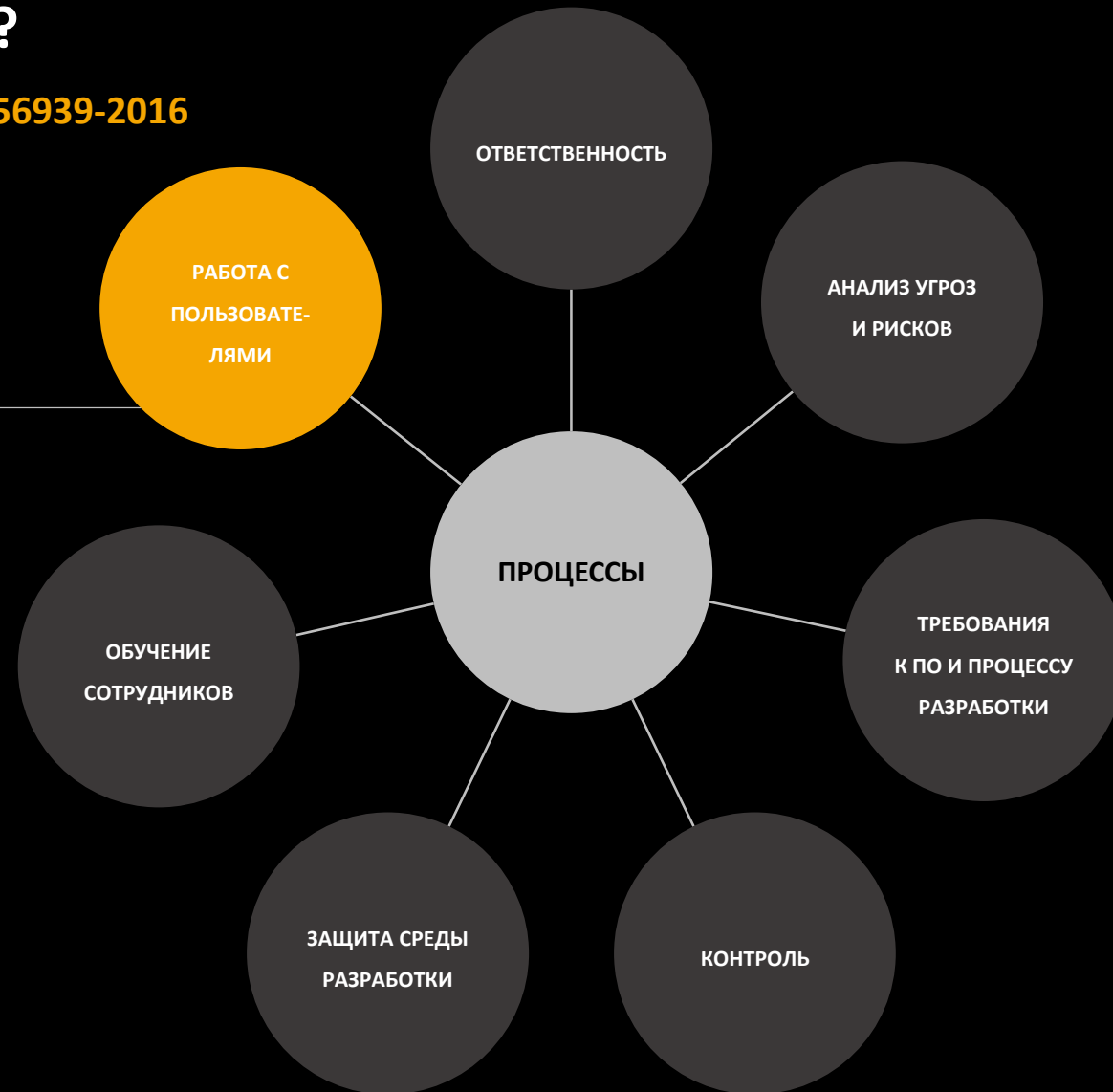


- повышение компетенций разработчиков в сфере ИБ
- пересмотр и доработка процесса разработки ПО

КАК ЭТО СДЕЛАТЬ?

В СООТВЕТСТВИИ С ГОСТ Р 56939-2016

- прием обращений об ошибках и уязвимостях
- уведомление пользователей



КАК ЭТО СДЕЛАТЬ?

ИНСТРУМЕНТЫ. УГРОЗЫ

Выявление:

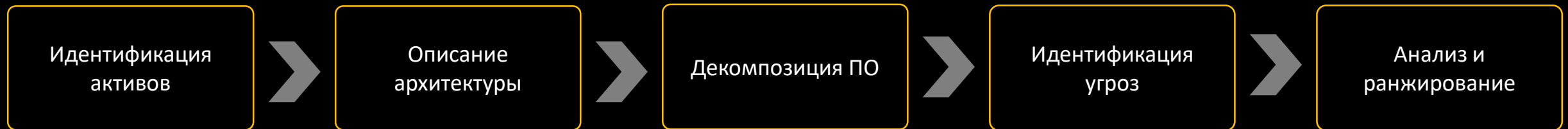
- угроз ИБ для ПО
- рисков ИБ в процессе разработки ПО

КАК ЭТО СДЕЛАТЬ?

ИНСТРУМЕНТЫ. УГРОЗЫ

Выявление:

- угроз ИБ для ПО
- рисков ИБ в процессе разработки ПО

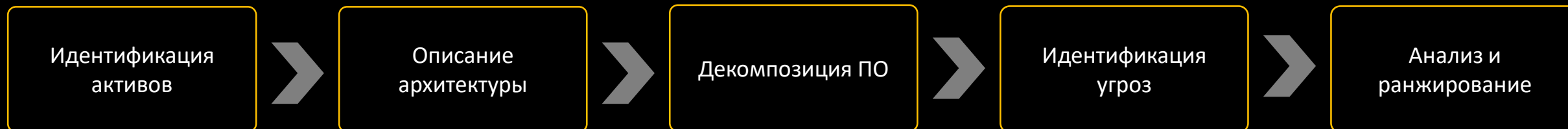


КАК ЭТО СДЕЛАТЬ?

ИНСТРУМЕНТЫ. УГРОЗЫ

Выявление:

- угроз ИБ для ПО
- рисков ИБ в процессе разработки ПО



Пример:

OWASP

Agile Threat Modeling Toolkit

MITRE ATT&CK for CI/CD

PyTM

STRIDE

КАК ЭТО СДЕЛАТЬ?

ИНСТРУМЕНТЫ. СТАТИЧЕСКИЙ АНАЛИЗ

Автоматизированный процесс обзора кода для выявления:

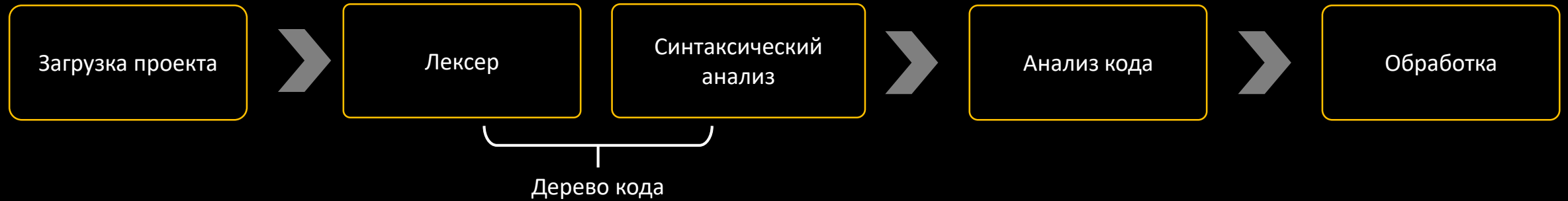
- ошибок
- дефектов
- уязвимостей

КАК ЭТО СДЕЛАТЬ?

ИНСТРУМЕНТЫ. СТАТИЧЕСКИЙ АНАЛИЗ

Автоматизированный процесс обзора кода для выявления:

- ошибок
- дефектов
- уязвимостей

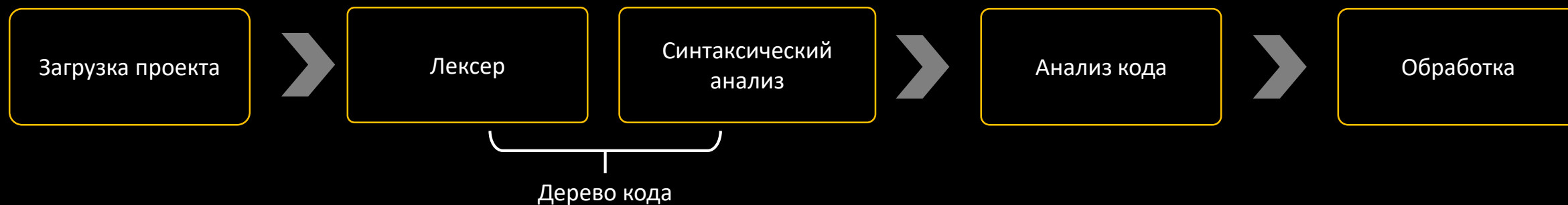


КАК ЭТО СДЕЛАТЬ?

ИНСТРУМЕНТЫ. СТАТИЧЕСКИЙ АНАЛИЗ

Автоматизированный процесс обзора кода для выявления:

- ошибок
- дефектов
- уязвимостей



Пример:

AppChecker

PT Application Inspector

PVS-Studio

Solar appScreener

КАК ЭТО СДЕЛАТЬ?

ИНСТРУМЕНТЫ. ДИНАМИЧЕСКИЙ АНАЛИЗ

Анализ кода при его исполнении для выявления:

- сложных ошибок (деление на ноль, утечка памяти и др.)
- необнаруженных ранее уязвимостей

КАК ЭТО СДЕЛАТЬ?

ИНСТРУМЕНТЫ. ДИНАМИЧЕСКИЙ АНАЛИЗ

Анализ кода при его исполнении для выявления:

- сложных ошибок (деление на ноль, утечка памяти и др.)
- необнаруженных ранее уязвимостей

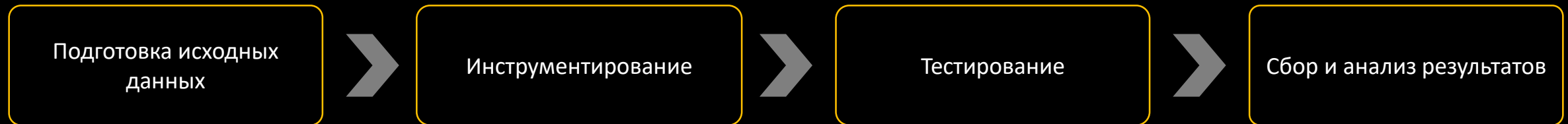


КАК ЭТО СДЕЛАТЬ?

ИНСТРУМЕНТЫ. ДИНАМИЧЕСКИЙ АНАЛИЗ

Анализ кода при его исполнении для выявления:

- сложных ошибок (деление на ноль, утечка памяти и др.)
- необнаруженных ранее уязвимостей



Пример:

PT Application Inspector

PT BlackBox

Burb Suite

Synopsys Managed DAST

КАК ЭТО СДЕЛАТЬ?

ИНСТРУМЕНТЫ. ФАЗЗИНГ-ТЕСТИРОВАНИЕ

Подача на вход ПО случайных или специально подготовленных данных, которые могут привести к нарушению работы ПО:

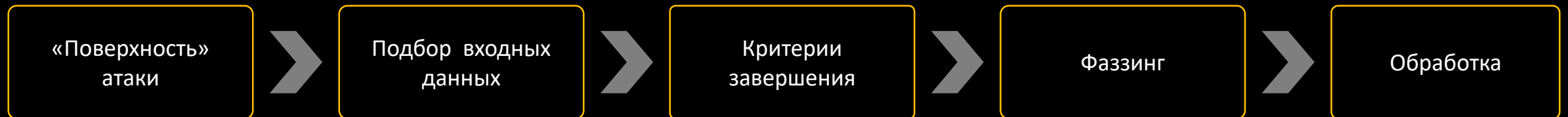
- аварийное состояние
- непрогнозируемое поведение

КАК ЭТО СДЕЛАТЬ?

ИНСТРУМЕНТЫ. ФАЗЗИНГ-ТЕСТИРОВАНИЕ

Подача на вход ПО случайных или специально подготовленных данных, которые могут привести к нарушению работы ПО:

- аварийное состояние
- непрогнозируемое поведение

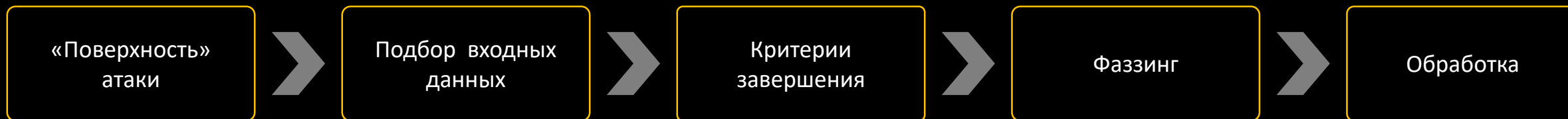


КАК ЭТО СДЕЛАТЬ?

ИНСТРУМЕНТЫ. ФАЗЗИНГ-ТЕСТИРОВАНИЕ

Подача на вход ПО случайных или специально подготовленных данных, которые могут привести к нарушению работы ПО:

- аварийное состояние
- непрогнозируемое поведение



ОПРОС №2

**Каким классом инструментов
вы пользуетесь при разработке?**

КАК ЭТО СДЕЛАТЬ?

люди

Application Security специалист



Разработчик
+ курсы по ИБ

Специалист по ИБ
+ курсы по разработке ПО

УЦСБ SSDLC

Разработчики



Оценка выполнения требований п.29.3 Приказа ФСТЭК России №239



Проверка ПО на наличие НДВ и уязвимостей



Внедрение инструментов по проверке ПО



Проверка Open Source компонентов и библиотек на наличие уязвимостей

Субъекты КИИ



Выполнение требований п.29.3 Приказа ФСТЭК России №239



Проверка ПО на наличие уязвимостей



Мониторинг инцидентов ИБ

Практические кейсы

ПРОВЕДЕНИЕ РАБОТ ПО ОЦЕНКЕ ПРОЦЕССОВ РАЗРАБОТКИ И РАЗРАБАТЫВАЕМОГО ПО В РАМКАХ 239 ПРИКАЗА ФСТЭК

ЗАКАЗЧИК

Разработчик SCADA платформы

ОСОБЕННОСТИ

1. Не просто SCADA, а среда разработки и автоматизации процессов АСУ ТП
2. Объем исходного кода превышает 150 ГБ
3. Многомодульная система, где каждый модуль требует анализа

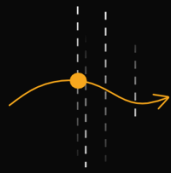
РЕЗУЛЬТАТ

1. Проведено комплексное обследование процессов разработки
2. «Под ключ» разработаны все необходимые документы
3. В рамках обследования был выявлен ряд уязвимостей, который Заказчик оперативно устранил
4. Подготовлены рекомендации для повышения зрелости процессов безопасной разработки

ПРОЦЕСС ПРОВЕДЕНИЯ АУДИТА

ГОСТ Р 56939-2016 Защита информации.

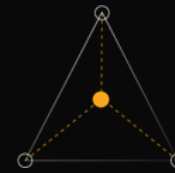
Разработка безопасного программного обеспечения



Подготовка опросных
листов



Проведение интервью
с командами разработки





Архитектурное ревью





Формирование
рекомендаций


ПОСТРОЕНИЕ МОДЕЛИ УГРОЗ


Анализ архитектуры
и функциональных
возможностей ПО 

Инвентаризация компонентов
и внешних сущностей ПО 

Определение потоков
данных между
компонентами ПО 

Определение поверхности
атак потенциального
нарушителя 

Выявлены потенциальные
угрозы безопасности ПО 

Рассмотрены способы
реализации угроз
и предложены меры по их
нейтрализации 

ПРОВЕДЕННЫЕ ИСПЫТАНИЯ

Статический анализ и фаззинг-тестирование



- Синтаксический анализ исходного кода и анализ путей выполнения
- Использование нескольких анализаторов и ручная верификация выявленных уязвимостей



- Выявление архитектурных уязвимостей с использованием мутационного фаззинга
- Ручное исследование частей приложений, в которых была вызвана ошибка при тестировании

ДАЛЬНЕЙШИЕ РАБОТЫ



Подключение к платформе непрерывного анализа защищенности ПО:

- Статический анализ
- Фаззинг-тестирование
- Динамический анализ
- Композиционный анализ



Сертификация разрабатываемого ПО в соответствии с Приказом ФСТЭК №76



- Сертификация процессов разработки в соответствии с Приказом ФСТЭК №240
- Сертификация процессов разработки ПО СЗИ

ОЗНАКОМЬТЕСЬ С ДРУГИМИ КЕЙСАМИ

1 Как анализ защищенности программного обеспечения помог **Банку Синара** выпустить надежный сервис по инвестициям

[Читать](#)



2 Как аудит процесса разработки помог группе **Ctrl2GO** успешно сдать проект и улучшить DevSecOps

[Читать](#)











3 Безопасное ПО для автоматизации значимых объектов КИИ — миссия выполнима, кейс с компанией **Атомик Софт**

[Читать](#)

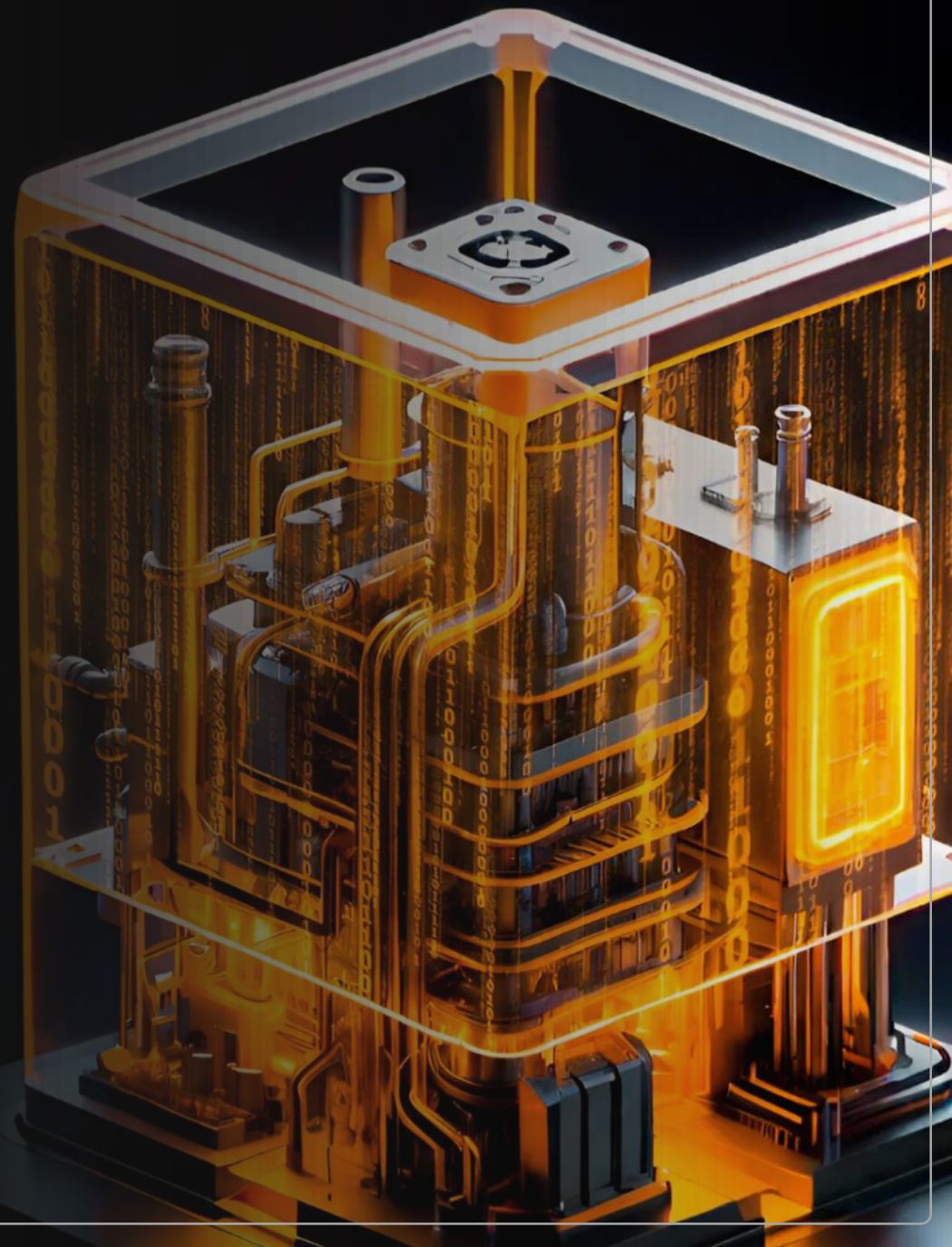


ПРОГРАММА ВЕБИНАРОВ

- 19.03  Как защитить КИИ от киберугроз? (Категорирование КИИ)
- 09.04  Как построить эффективную систему обеспечения ИБ объектов КИИ
- 25.04  Практика построения СОИБ: проблемы, решения, кейсы
- 28.05  Мониторинг инцидентов ИБ ОКИИ
- 04.06  РАМ или пропал: как обеспечить эффективное управление привилегированным доступом для защиты КИИ
- 09.07  Безопасная разработка ПО для значимых объектов КИИ
- 01.08  Как оценить защищенность ЗОКИИ и почему пентесты — эффективный инструмент
-  Подготовка к прохождению госконтроля

Подписывайтесь на наш канал в Телеграме

- Ежемесячные обзоры изменения законодательства
- Разбор часто задаваемых вопросов по теме КИИ
- Экспертные статьи и кейсы





СПАСИБО ЗА ВНИМАНИЕ! ВОПРОСЫ?

Станислав Соболев

Старший инженер по безопасности приложений

Евгений Тодышев

Руководитель направления безопасной разработки

2024

sec@ussc.ru

sec.ussc.ru

