Kaspersky Industrial Cybersecurity Conference 2019

September 18-20, 2019, Sochi, Russia

kaspersky

Before the War: киберучения и пентест в АСУ ТП

Виталий Сиянов

Руководитель направления защиты АСУ ТП

«Инфосистемы Джет»

va.siyanov@jet.su | +7 926 629 13 23

AGENDA

- Виды пентеста
- Особенности пентеста в АСУ ТП
- Кому нужны киберучения
- Пример киберучений
- Выводы

ОБЩАЯ ИНФОРМАЦИЯ

Тестирование на проникновение (Pentest)

Эмуляция действий реальных злоумышленников, использование тех же векторов атак, инструментов и последовательностей действий, которые используют злоумышленники в реальных атаках

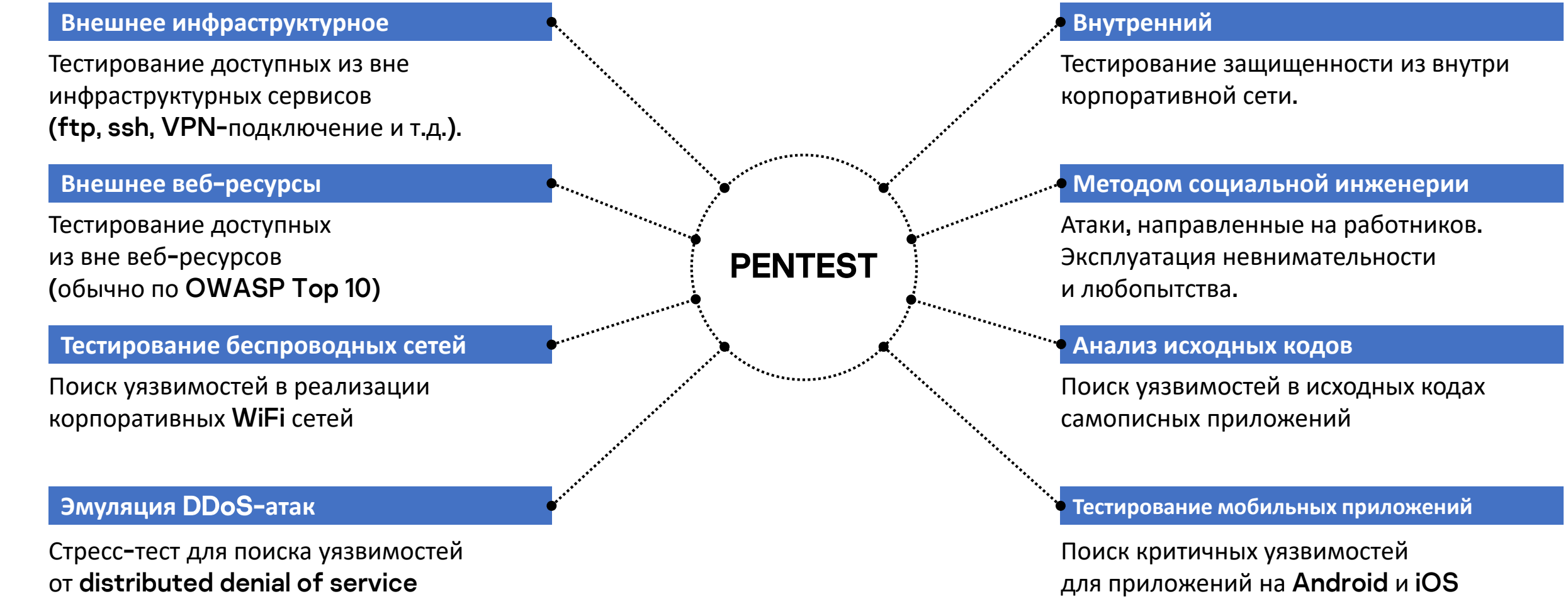
Анализ защищенности

Процесс проверки инфраструктуры организации на наличие возможных уязвимостей сетевого периметра, виртуальной инфраструктуры, вызванных в том числе ошибками конфигурации, а также программного обеспечения и исходного кода приложений

Кто

Этичные хакеры – **«WhiteHat».** Работники компаний, специализирующихся на оказании услуг в области информационной безопасности

ВИДЫ ТЕСТИРОВАНИЙ НА ПРОНИКНОВЕНИЕ



Внешнее инфраструктурное

Тестирование доступных из вне инфраструктурных сервисов **(ftp, ssh, VPN-**подключение и т.д.**).**

Внешнее веб-ресурсы

Тестирование доступных из вне веб-ресурсов (обычно по **OWASP Top 10**)

Тестирование беспроводных сетей

Поиск уязвимостей в реализации корпоративных **WiFi** сетей

Эмуляция DDoS-атак

Стресс-тест для поиска уязвимостей от **distributed denial of service**

Внутренний

Тестирование защищенности из внутри корпоративной сети.

Методом социальной инженерии

Атаки, направленные на работников. Эксплуатация невнимательности и любопытства.

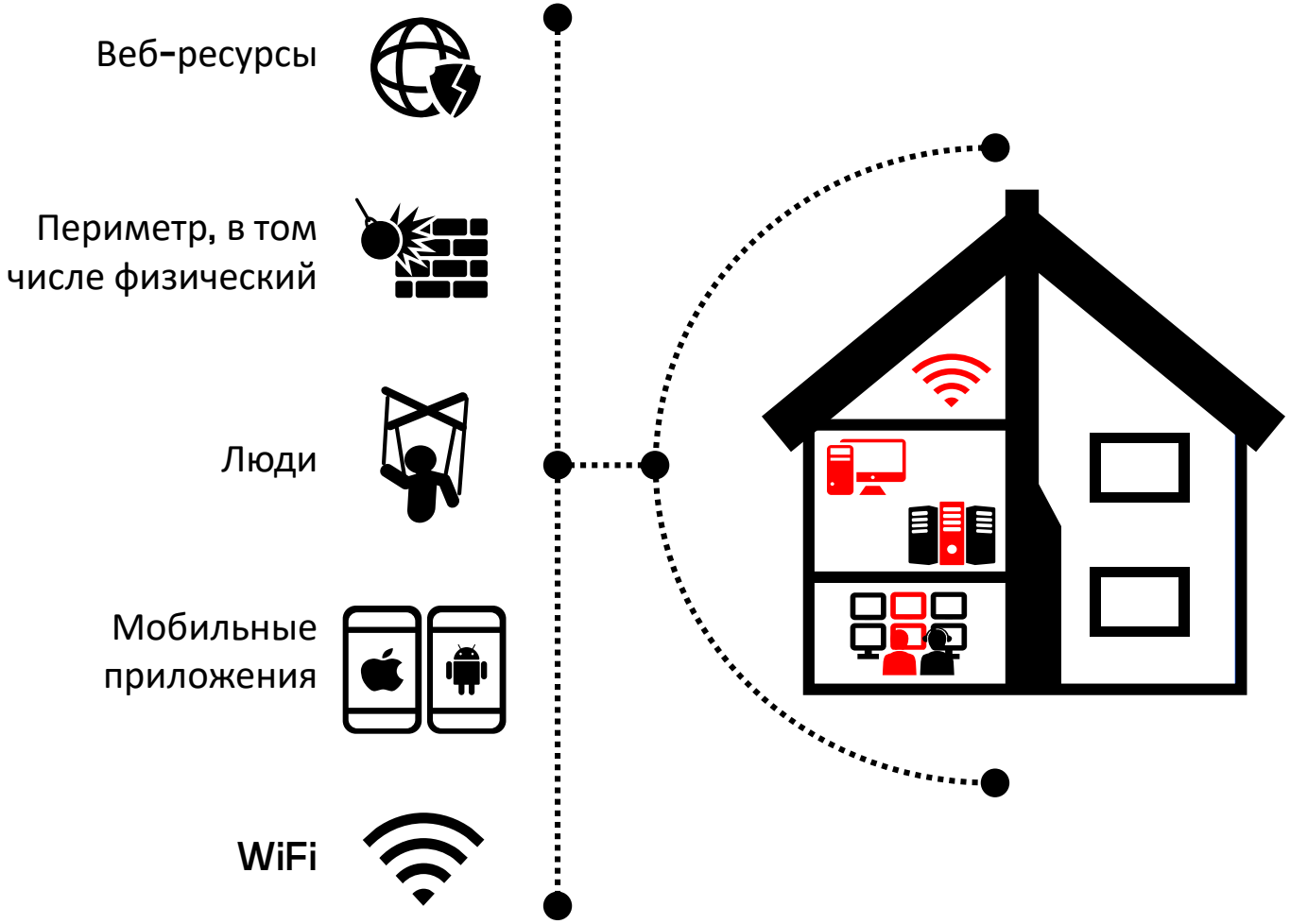
Анализ исходных кодов

Поиск уязвимостей в исходных кодах самописных приложений

Тестирование мобильных приложений

Поиск критичных уязвимостей для приложений на **Android** и **iOS**

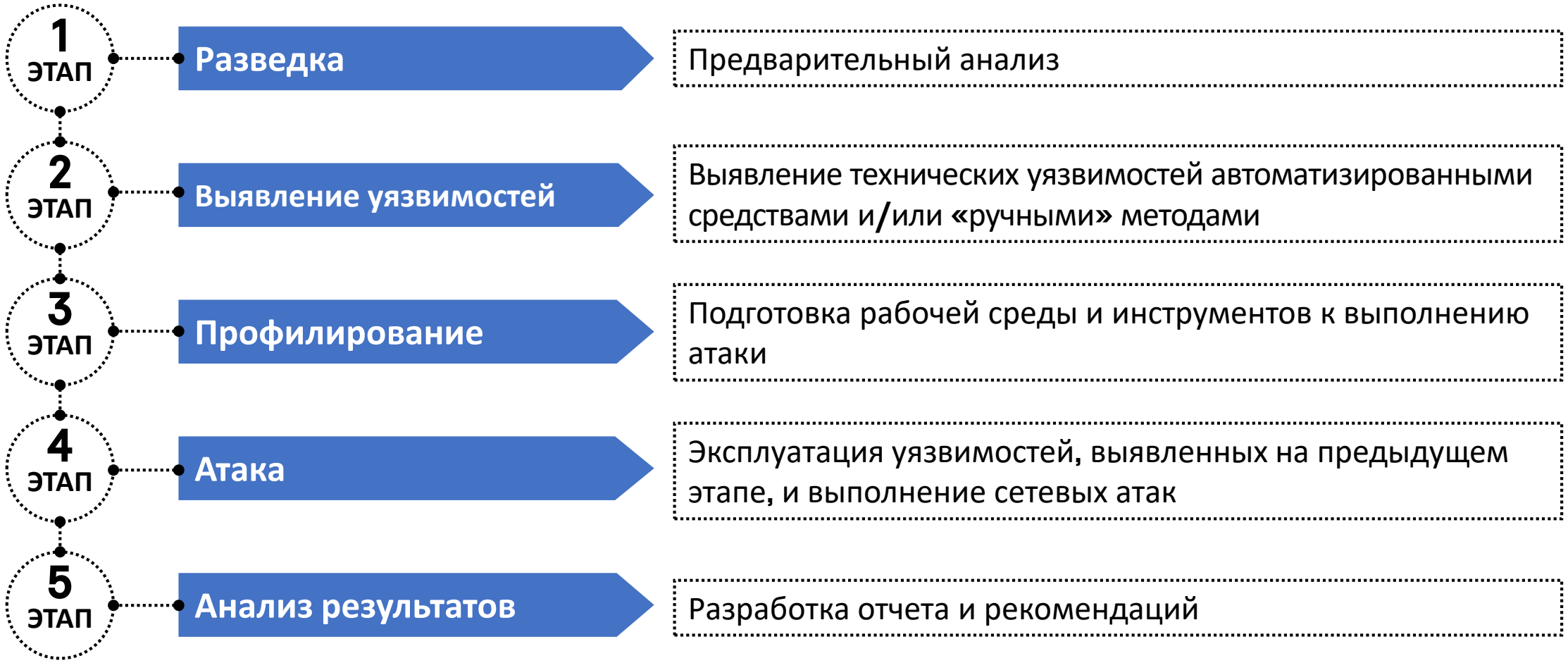
ЦЕЛЕНАПРАВЛЕННАЯ АТАКА – RED TEAM



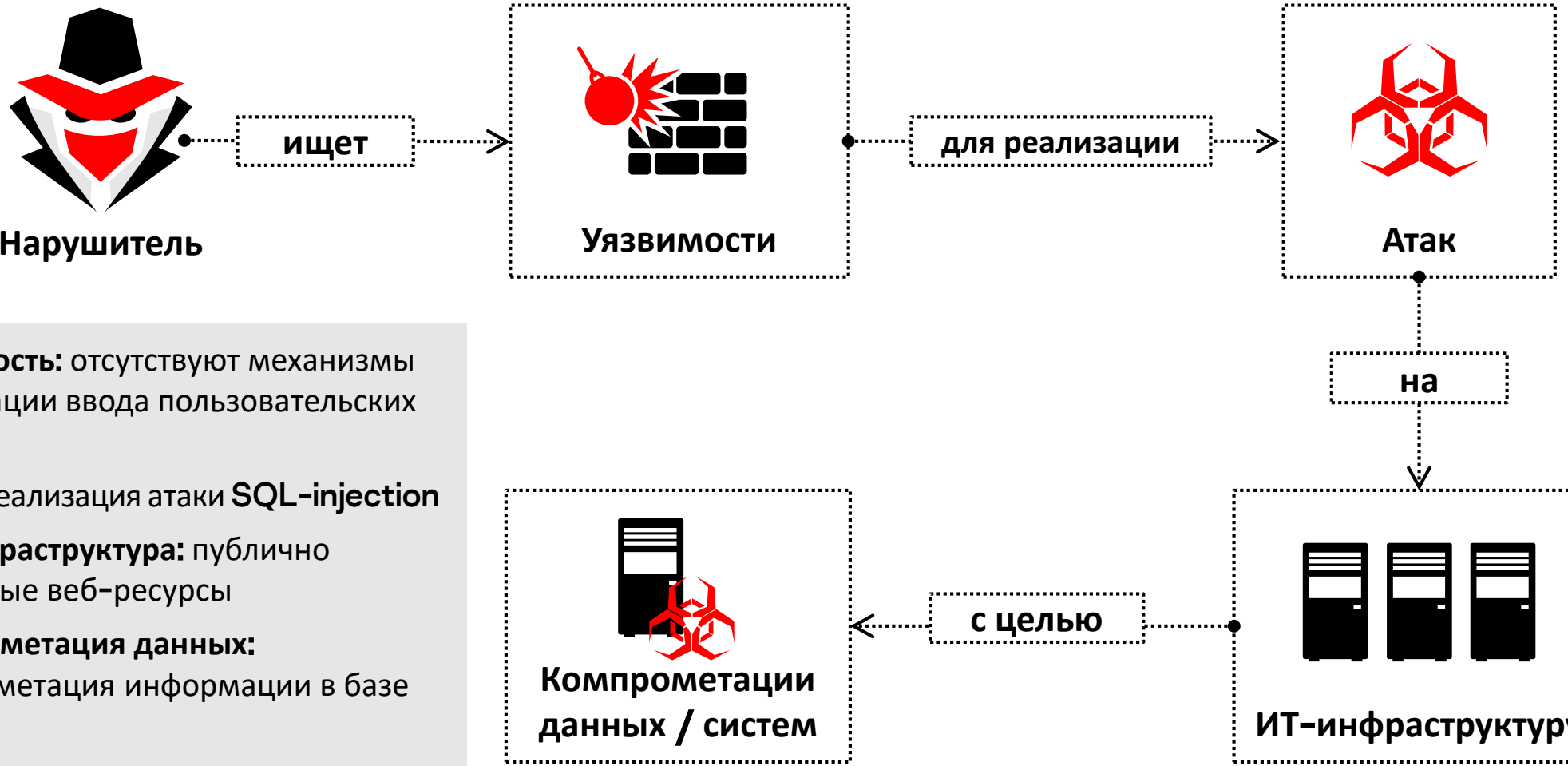
ОСОБЕННОСТИ

- Атаки на удаленные предприятия и доп. офисы
- Атаки через периферийное оборудование
- Атаки типа **Dumpster Diving** (поиск информации в мусоре)
- Атаки на физический периметр на различных площадках
- Атаки через третьи стороны
- **Расширенная** социальная инженерия

ХОД ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ



ПРИМЕР АТАКИ



Уязвимость: отсутствуют механизмы фильтрации ввода пользовательских данных

Атака: реализация атаки **SQL-injection**

ИТ-инфраструктура: публично доступные веб-ресурсы

Компрометация данных: компрометация информации в базе данных

Не надо делать из шахты склеп…

Цитата заказчика во время пентеста

ОСОБЕННОСТИ ПЕНТЕСТА (АНАЛИЗА ЗАЩИЩЕННОСТИ) В АСУ ТП

Особенности

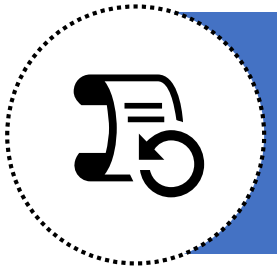
- Тестирование специализированных протоколов
- Осторожное сканирование
- Создание «стендов» для тестирования или во время останова
- Специализированные рекомендации по устранению выявленных уязвимостей
- Закрытие уязвимостей компенсирующими мерами

Ограничения пентестов

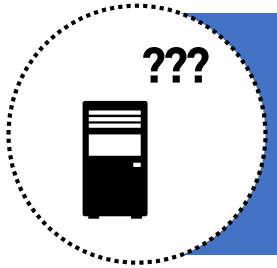
- Зачастую устаревшее оборудование, которое не обновляется
- Установки управляют физическими процессами, как следствие повышается цена ошибки
- Условная изоляция технологической сети от корпоративной
- Угроза выхода оборудования из строя про пентесте
- Каждый пентест АСУ ТП будет уникальным

ВЫВОДЫ

Проводите пентест на стендах или во время останова



Заранее пропишите каждый шаг и моменты согласования



Учитывайте особенности оборудования

Привлекайте пентестеров с опытом тестирования технологических сетей

КИБЕРУЧЕНИЯ

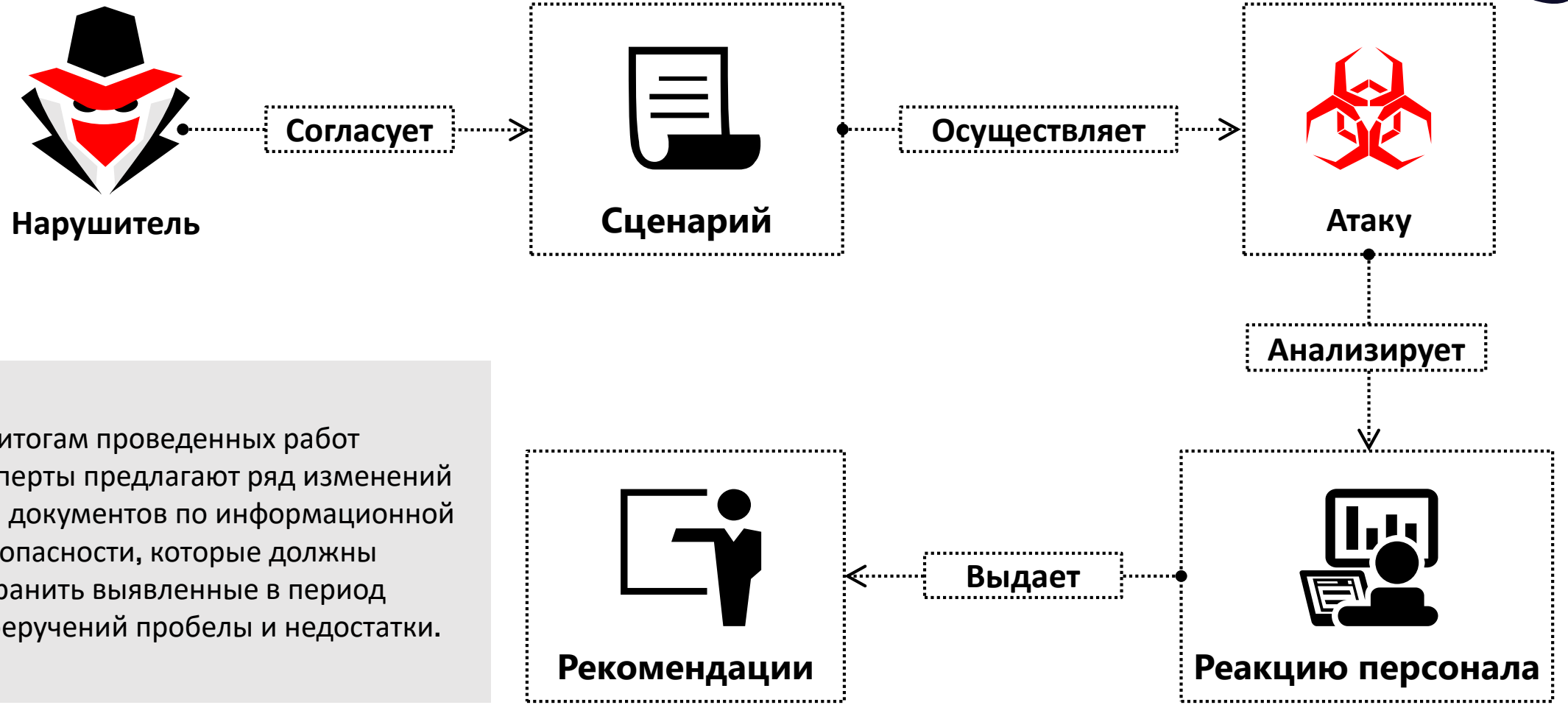
Киберучения — это инструмент повышения готовности компании к нештатным ситуациям и обнаружения слабых мест в защите компании.

Киберучения направлены на проверку знаний своих обязанностей персоналом и умение действовать в критической ситуации, отработку взаимодействия подразделений и анализ актуальности требований, прописанных в инструкциях и регламентах предприятия. По итогам проведенных киберучений готовится отчет об уязвимостях, обнаруженных при выполнении работ, и корректируются документы по информационной безопасности.

Приказ ФСТЭК №239 от 25 декабря 2017 года

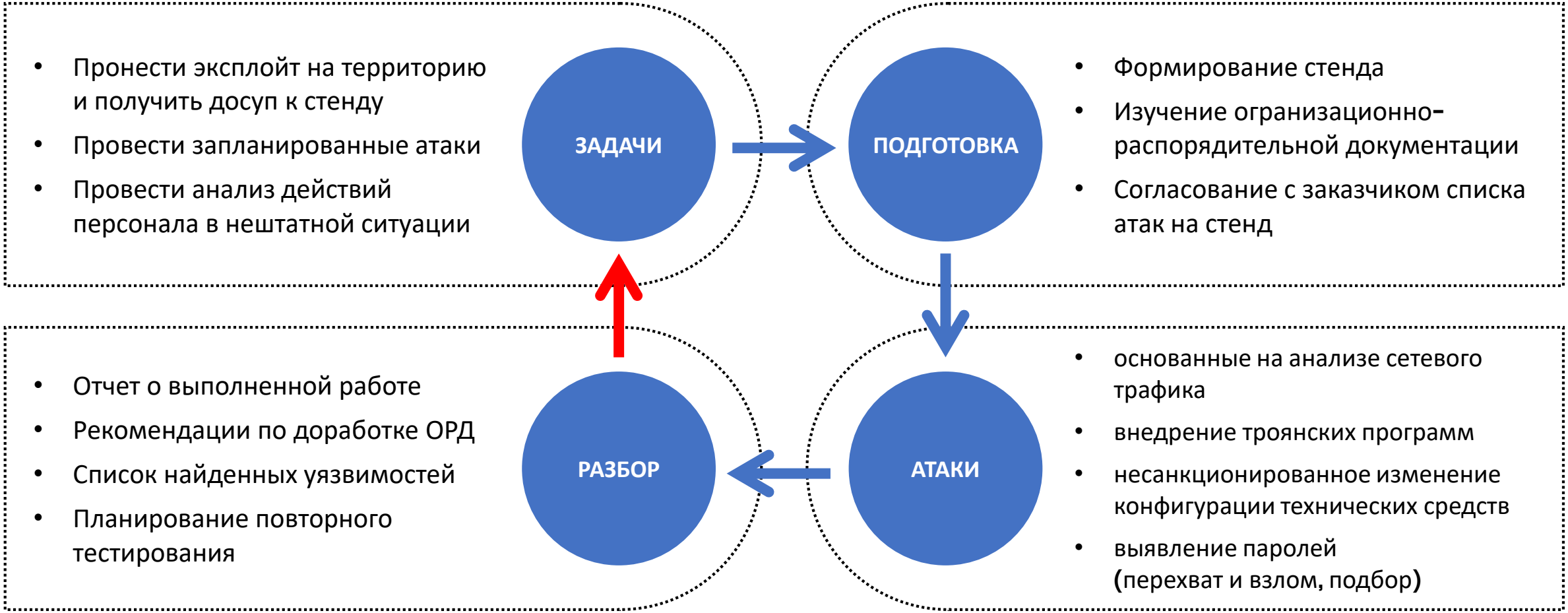
Раздел **XVII.** Информирование и обучение персонала (ИПО)
ИПО **3.** Проведение практических занятий с персоналом по правилам безопасной работы

ПРИМЕР КИБЕРУЧЕНИЙ



По итогам проведенных работ эксперты предлагают ряд изменений для документов по информационной безопасности, которые должны устранить выявленные в период киберучений пробелы и недостатки.

ПРИМЕРНЫЙ СЦЕНАРИЙ КИБЕРУЧЕНИЙ



- Пронести эксплойт на территорию и получить досуп к стенду
- Провести запланированные атаки
- Провести анализ действий персонала в нештатной ситуации

- Формирование стенда
- Изучение огранизационно-распорядительной документации
- Согласование с заказчиком списка атак на стенд

- основанные на анализе сетевого трафика
- внедрение троянских программ
- несанкционированное изменение конфигурации технических средств
- выявление паролей (перехват и взлом, подбор)

- Отчет о выполненной работе
- Рекомендации по доработке ОРД
- Список найденных уязвимостей
- Планирование повторного тестирования

Пример атаки на контроллер

Kaspersky Industrial Cybersecurity Conference 2019

September 18-20, 2019, Sochi, Russia

kaspersky

Thank you!

Виталий Сиянов

Руководитель направления защиты АСУ ТП

«Инфосистемы Джет»

va.siyanov@jet.su | +7 926 629 13 23