УЦСБ

Как оценить защищенность ОКИИ и почему **пентесты** – **эффективный инструмент**

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

УЦСБ

ПЛАН ВЕБИНАРА

01 Методы оценки защищенности

02 Требования нормативных документов

03 Виды услуг по пентесту

04 Этапы работ и практические кейсы

05 Как сделать результаты оценки эффективнее

УЦСБ

МЕТОДЫ ОЦЕНКИ ЗАЩИЩЕННОСТИ

Методами оценки могут быть:

- анализ документации по безопасности объекта
- периодическое сканирование на уязвимости
- анализ состава установленного программного обеспечения и обновлений
- анализ исходного кода
- анализ конфигураций программных и программно-аппаратных средств

Перечисленные методы не дают четкий ответ на вопросы:

? возможно ли нарушение работы ЗОКИИ реальным злоумышленником

? готов ли субъект КИИ к реальной атаке

ПЕНТЕСТ

Тестирование на проникновение (пентест)

Метод оценки мер обеспечения безопасности информационных систем, при котором возможность реализации рисков ИБ проверяется путем моделирования атак

Особенности:

- преобладание ручных проверок
- возможность оценить критичность уязвимостей с учетом контекста
- результатом является не только перечень уязвимостей, но и описание реализованных векторов атак
- может включать социотехнические проверки
- может включать оценку мер противодействия

УЦСБ

Требования к оценке защищенности, применимые к ЗОКИИ*

*за исключением требований по защите государственной тайны

Защита КИИ

Федеральный закон **№ 187-ФЗ**
Приказ ФСТЭК России **№ 235**
Приказ ФСТЭК России **№ 239**

Финансовая сфера

Положение ЦБ РФ **№ 683-П**
Положение ЦБ РФ **№ 821-П**
Положение ЦБ РФ **№ 757-П**

Указ Президента РФ № 250

Приказ ФСБ России **№ 213**
Постановление Правительства **№ 1272**
Типовое ТЗ от Минцифры

Государственные системы

Приказ ФСТЭК России **№ 17**
Постановление Правительства РФ **№ 860**

Персональные данные

Приказ ФСТЭК России **№ 21**

АСУ ТП

Приказ ФСТЭК России **№ 31**

- - - - - - - - - - проведение пентеста обязательно

- - - - - - - - - - проведение пентеста является одним из возможных методов оценки защищенности

Оценка защищенности по Указу Президента РФ № 250

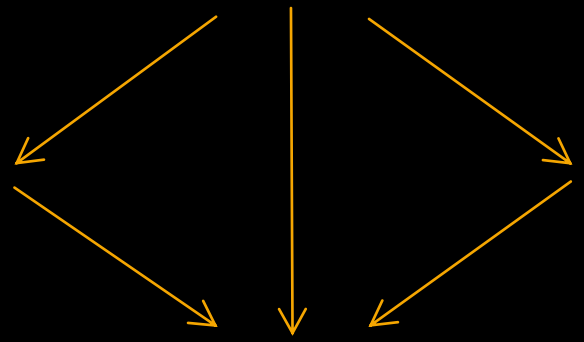
Указ Президента РФ № 250

На кого распространяется:
- федеральные органы исполнительной власти
- государственные фонды и организации
- стратегические и системообразующие организации
- субъекты КИИ (независимо от наличия ЗОКИИ)

Предусматривает разовую оценку защищенности для ключевых органов (организаций)

Постановление Правительства № 1272

- утверждены типовые положения о заместителе руководителя и о структурном подразделении, ответственными за обеспечение ИБ
- Положения предусматривают проведение оценки защищенности



Приказ ФСБ России № 213

- ФСБ России осуществляет непрерывный мониторинг защищенности ресурсов, доступных из сети Интернет
- На основании годового плана проводится оценка защищенности органов (организаций)

Типовые документы по оценке защищенности от Минцифры:
- Типовое ТЗ
- Типовая форма отчета для Правительства РФ
- Пример заполнения типовой формы отчета

УЦСБ

ТЗ МИНЦИФРЫ

Появилось в контексте Указа Президента №250 и носит рекомендательный характер

Предусматривает:

- создание реестра недопустимых событий (НС)
- проверку возможностей реализации НС
- оценку мер противодействия атакам
- разработку маршрутной карты по повышению уровня защищенности

Включает:

- неисчерпывающий перечень проверок для веб-приложений, внешних и внутренних ресурсов
- перечень задач, решаемых при оценке защищенности
- требования к отчетной документации

УЦСБ

ОПРОС №1

Используете ли вы типовое ТЗ Минцифры?

УЦСБ

ЧТО ТРЕБУЕТ ДОРАБОТКИ

- основной мотив ТЗ – проверка внешнего периметра
- рассматривается только одна модель нарушителя
- не рассматриваются методы социальной инженерии
- предъявляемые ТЗ требования не всегда актуальны

ТИПОВОЕ ТЕХНИЧЕСКОЕ ЗАДАНИЕ
НА ВЫПОЛНЕНИЕ РАБОТ ПО ОЦЕНКЕ УРОВНЯ ЗАЩИЩЕННОСТИ
ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Москва, 2022 г.

С ЧЕГО НАЧАТЬ?

- перечень НС
- объекты оценки:
  - ИТ-инфраструктура ЗОКИИ
  - смежные системы
  - ПО ЗОКИИ
  - пользователи
  - сотрудники служб мониторинга и реагирования на инциденты
- модели нарушителя
- содержание отчетности
- бюджет и сроки

УЦСБ

СРАВНЕНИЕ РАЗНЫХ ПОДХОДОВ К ОЦЕНКЕ ЗАЩИЩЕННОСТИ

	Особенности	Длительность	Результаты	Стоимость
Сканирование	Попытки проникновения не осуществляются	*	Перечень уязвимостей и рекомендации по устранению	$
Пентест	• Осуществляется проникновение в инфраструктуру • Защитники уведомлены и не вмешиваются	**	• Перечень уязвимостей и орг. недостатков и рекомендации по устранению • Описание реализованных векторов атак	$$
Red Team	• Осуществляется проникновение в инфраструктуру • Используются техники скрытности • Защитники не уведомлены и вмешиваются	****	• Перечень уязвимостей и орг. недостатков и рекомендации по устранению • Описание реализованных векторов атак • Оценка мер противодействия и рекомендации по повышению эффективности	$$$$
Purple Team	• Осуществляется проникновение в инфраструктуру • Используются техники скрытности • Защитники уведомлены и взаимодействуют с атакующими	***	• Перечень уязвимостей и орг. недостатков и рекомендации по устранению • Описание реализованных векторов атак • Оценка мер противодействия и рекомендации по повышению эффективности • Обратная связь в моменте	$$$

УЦСБ

Как выглядит оценка защищенности на практике

УЦСБ

ОРГАНИЗАЦИЯ РАБОТ

Организационная работа

Определение целей
и границ работ

Информирование НКЦКИ
о проведении работ

Подготовка УЗ, удаленного доступа,
стендов и допусков

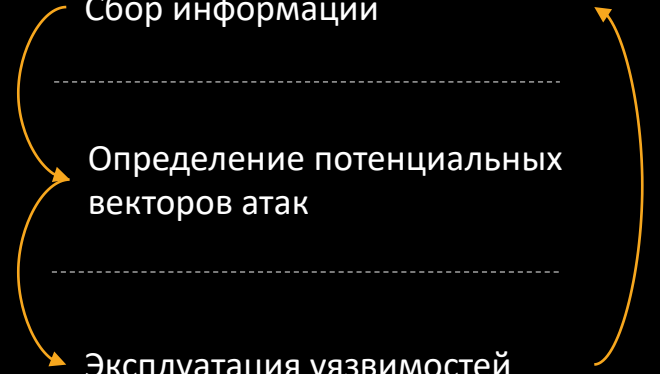
Согласование перечня проверок

Техническая работа

Сбор информации

Определение потенциальных
векторов атак

Эксплуатация уязвимостей



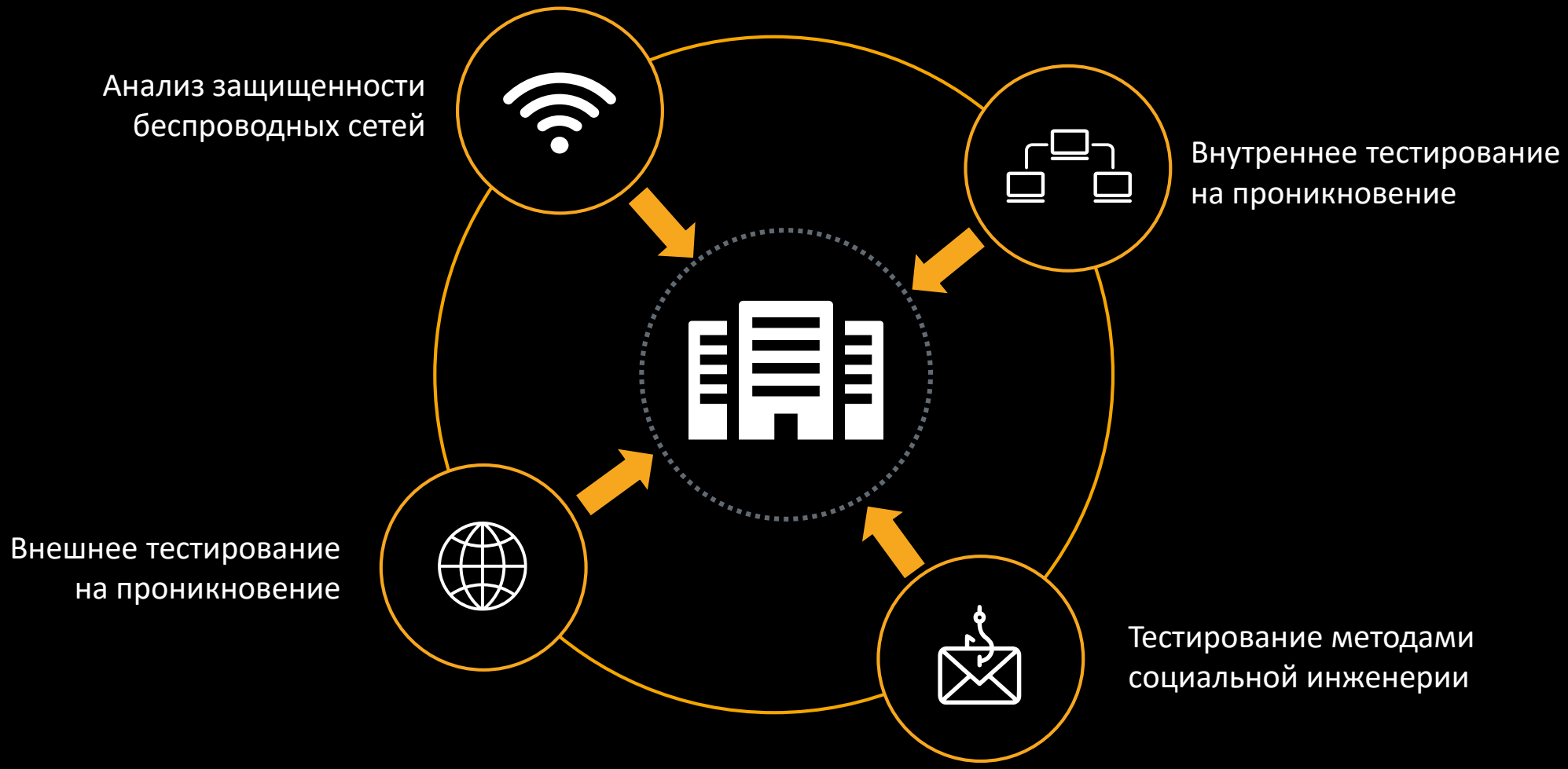
эти шаги могут
выполняться
последовательно
в несколько циклов

Восстановление исходного
состояния

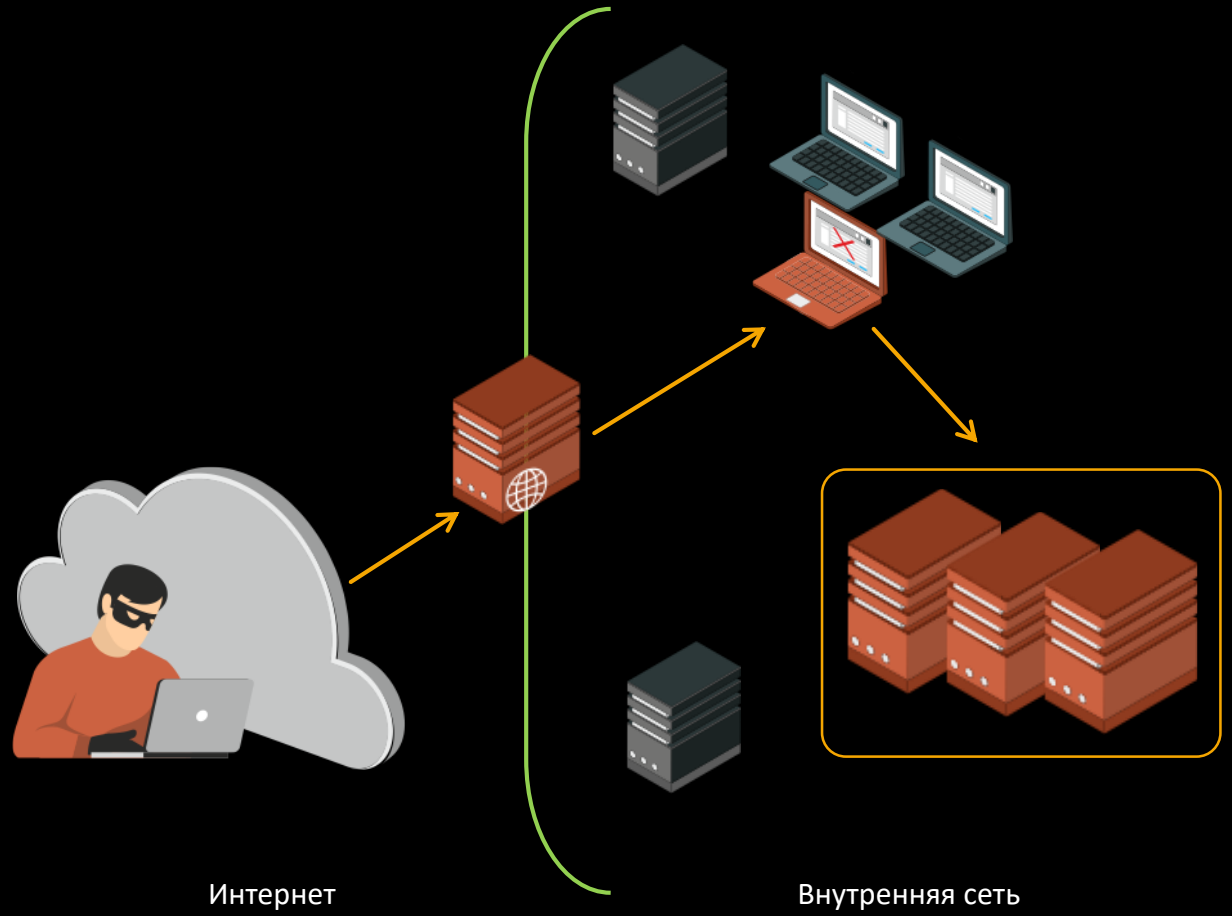
Разработка отчетной
документации

УЦСБ

ЭТАПЫ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ



ВНЕШНЕЕ ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ



- Проверяются возможности реализации НС и получения доступа к внутренним ресурсам снаружи
- Работы проводятся в согласованные временные промежутки через Интернет
- Проверки выполняются вручную

УЦСБ

ВНЕШНЕЕ ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ

Часто встречающиеся проблемы:

- доступ к почтовым службам
- небезопасные конфигурации Bitrix
- небезопасные веб-приложения
- избыточно опубликованные сервисы
- отсутствие мониторинга и СЗИ
- отсутствие изоляции внутренней сети

Примеры:

- сервер Exchange без мониторинга и WAF
- IP-камеры, доступные на внешнем периметре промышленного предприятия
- размещенный внутри периметра сайт предприятия с SQL-инъекцией
- доступный снаружи сервер 1С, включенный в домен AD
- доступный по прямой ссылке архив с персональными данными

ПРИМЕР: ДОСТУП ВО ВНУТРЕННЮЮ СЕТЬ ЧЕРЕЗ СЕРВЕР 1С

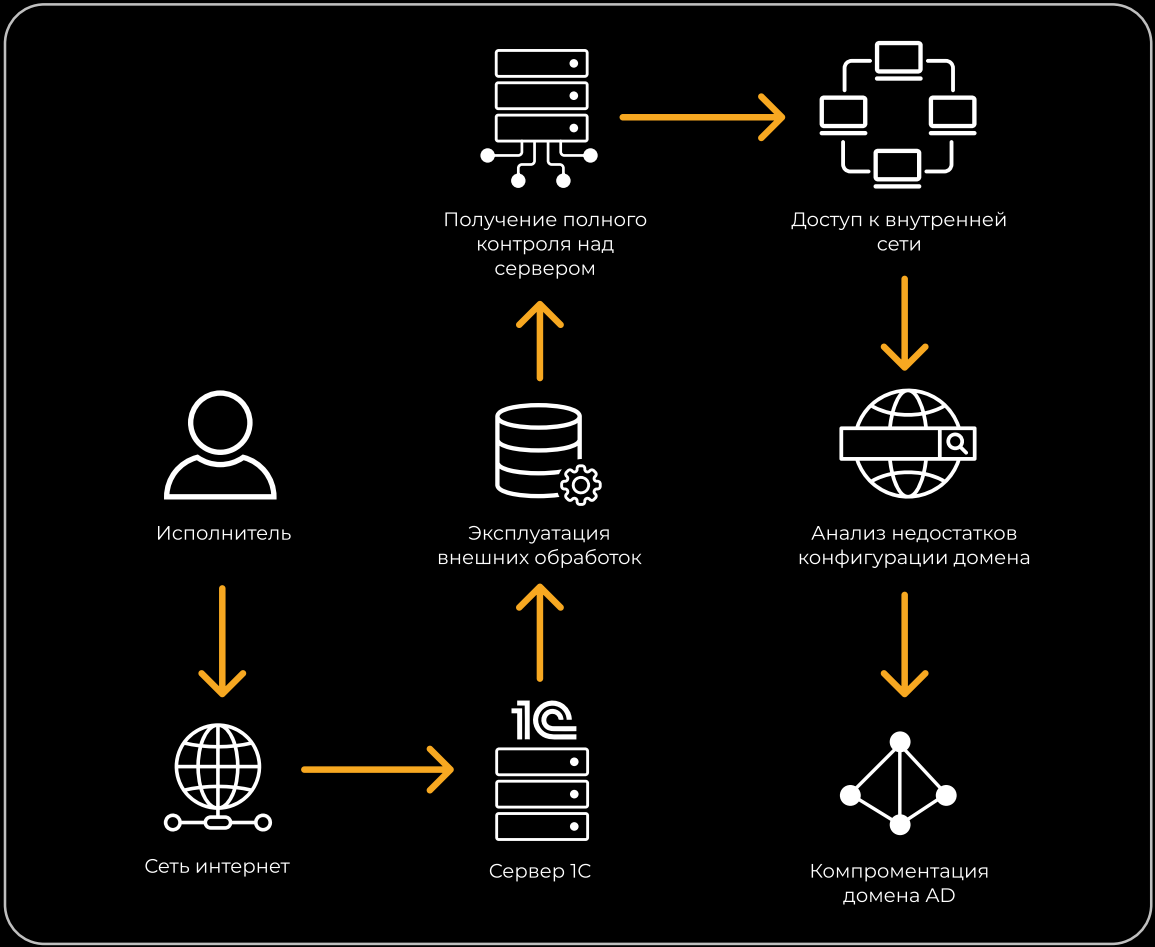
МОДЕЛЬ НАРУШИТЕЛЯ:
ВНЕШНИЙ НАРУШИТЕЛЬ, НЕ ИМЕЮЩИЙ ЛЕГИТИМНОГО ДОСТУПА К РЕСУРСАМ

Шаг 1. Обнаружили сервер 1С с автоматическим входом от имени администратора

Шаг 2. С помощью внешних обработок на сервере выполнили команды, получили полный контроль над сервером

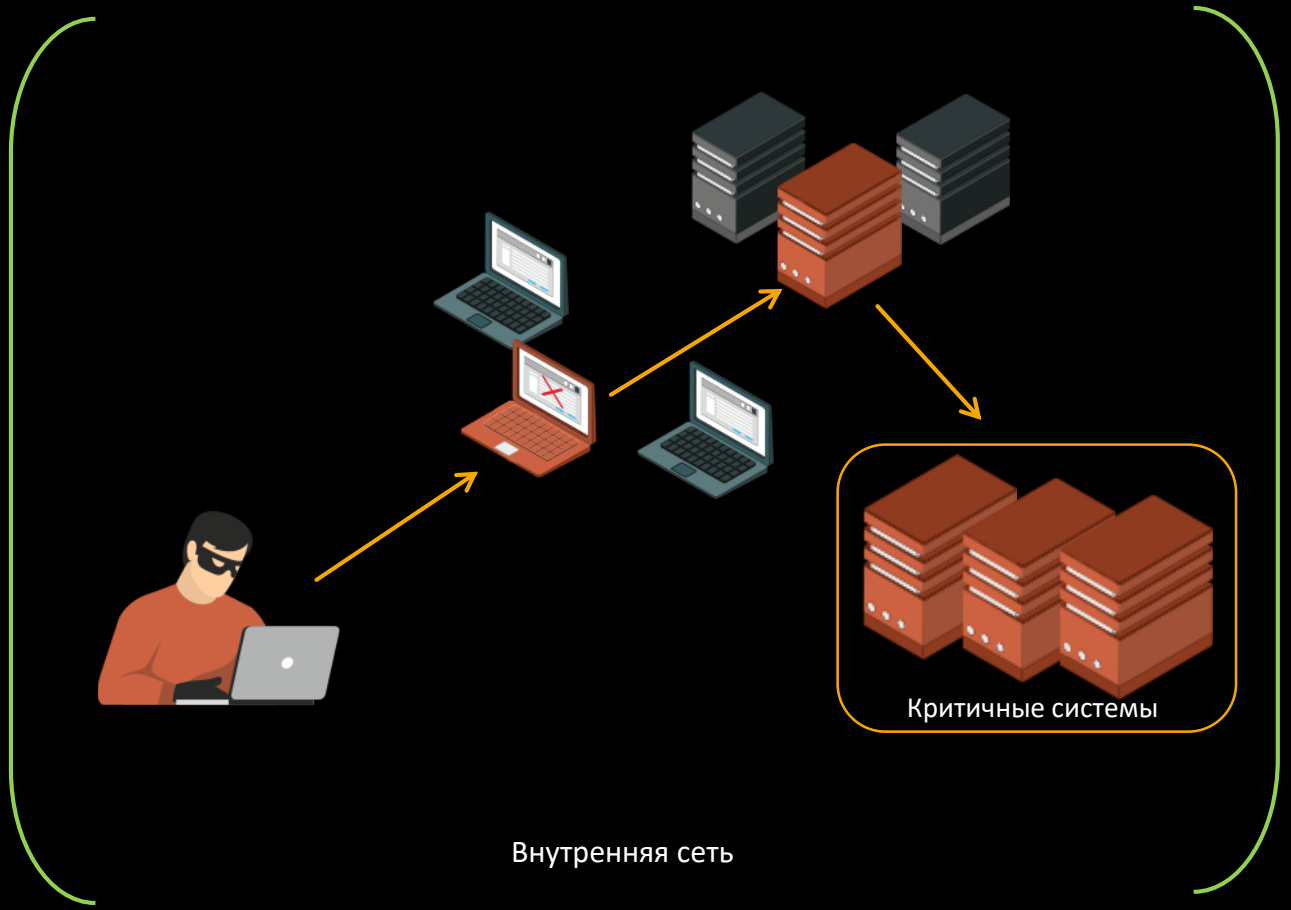
Шаг 3. Использовали сервер для доступа к внутренней сети, провели анализ домена Active Directory

Шаг 4. Использовали выявленные недостатки в конфигурации домена для получения привилегий администратора домена



УЦСБ

ВНУТРЕННЕЕ ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ



- Проверяются возможности реализации НС и получения доступа к критичным системам изнутри
- Работы проводятся очно на объекте или с использованием удаленного доступа
- Проверки выполняются вручную

УЦСБ

ВНУТРЕННЕЕ ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ

Часто встречающиеся проблемы:

- отсутствие обновлений безопасности
- недостаток мониторинга и СЗИ
- ошибки конфигурации систем
- организационные недостатки
- недостаточное сегментирование сети
- нарушения парольных политик

Примеры:

- небезопасная конфигурация ADCS
- избыточные права пользователей домена AD
- повторное использование паролей локальных администраторов
- использование словарных паролей
- доступ к серверным подсетям из пользовательского сегмента
- уязвимости систем виртуализации и резервного копирования
- забытые серверы и рабочие станции

УЦСБ

ПРИМЕР: ПОВТОРНОЕ ИСПОЛЬЗОВАНИЕ ПАРОЛЕЙ И ADCS

МОДЕЛЬ НАРУШИТЕЛЯ:
ГОСТЬ В ОФИСЕ

Шаг 1. Нашли в переговорной ноутбук, подключенный к гостевой сети Wi-Fi и к проводной корпоративной сети

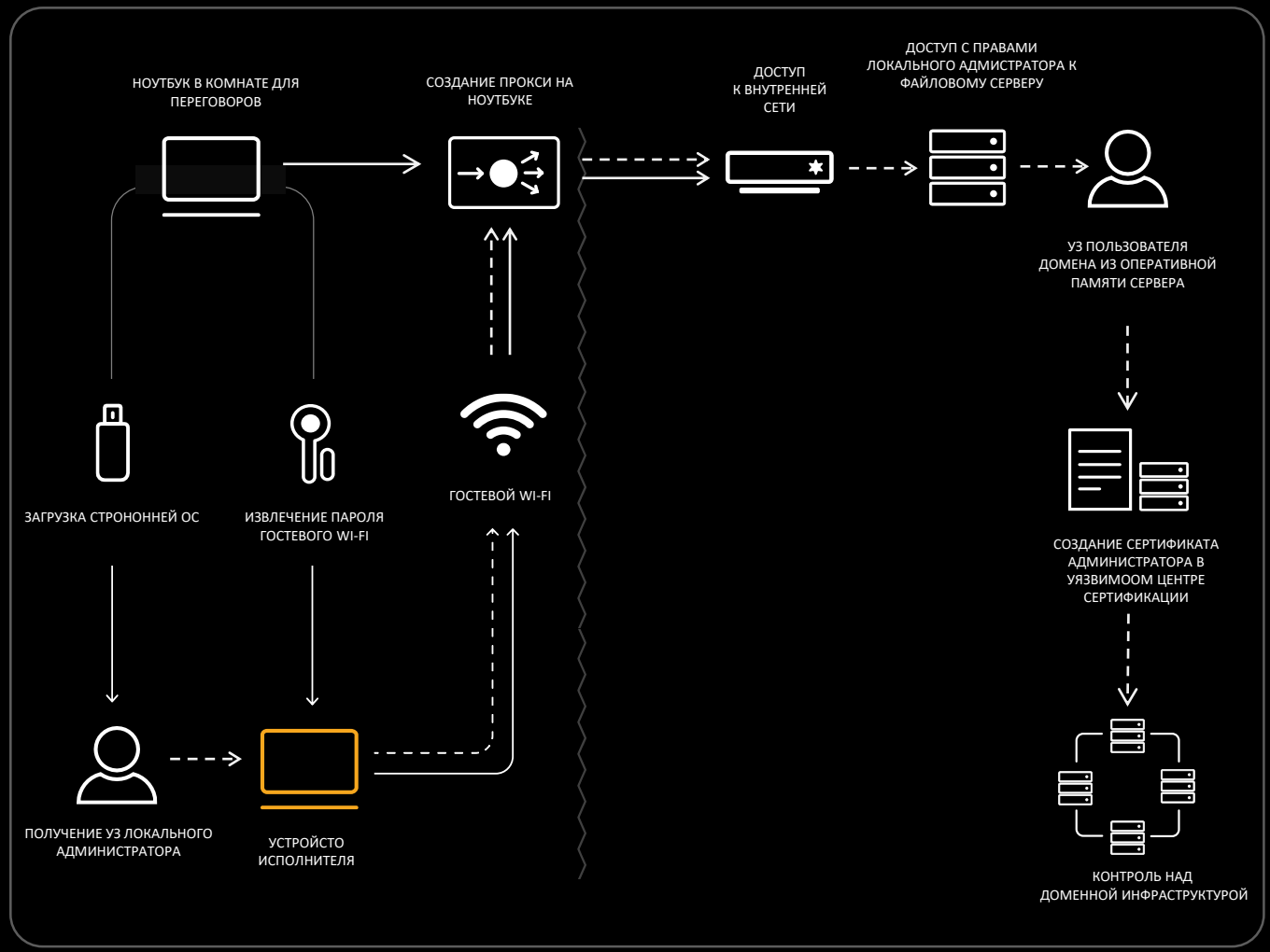
Шаг 2. Загрузили ноутбук с загрузочного USB и извлекли хэш локального администратора

Шаг 3. Перезагрузили ноутбук, извлекли из настроек пароль для подключения к Wi-Fi и настроили прокси в проводную корпоративную сеть

Шаг 4. Хэш локального администратора ноутбука позволил получить доступ к файловому серверу с правами локального администратора. Из памяти сервера извлекли учетные данные доменной УЗ

Шаг 5. Используя доменную УЗ, воспользовались ошибкой конфигурации ADCS и выпустили сертификат на имя администратора домена

Шаг 6. С помощью полученного сертификата продемонстрировали доступ ко всем устройствам в домене



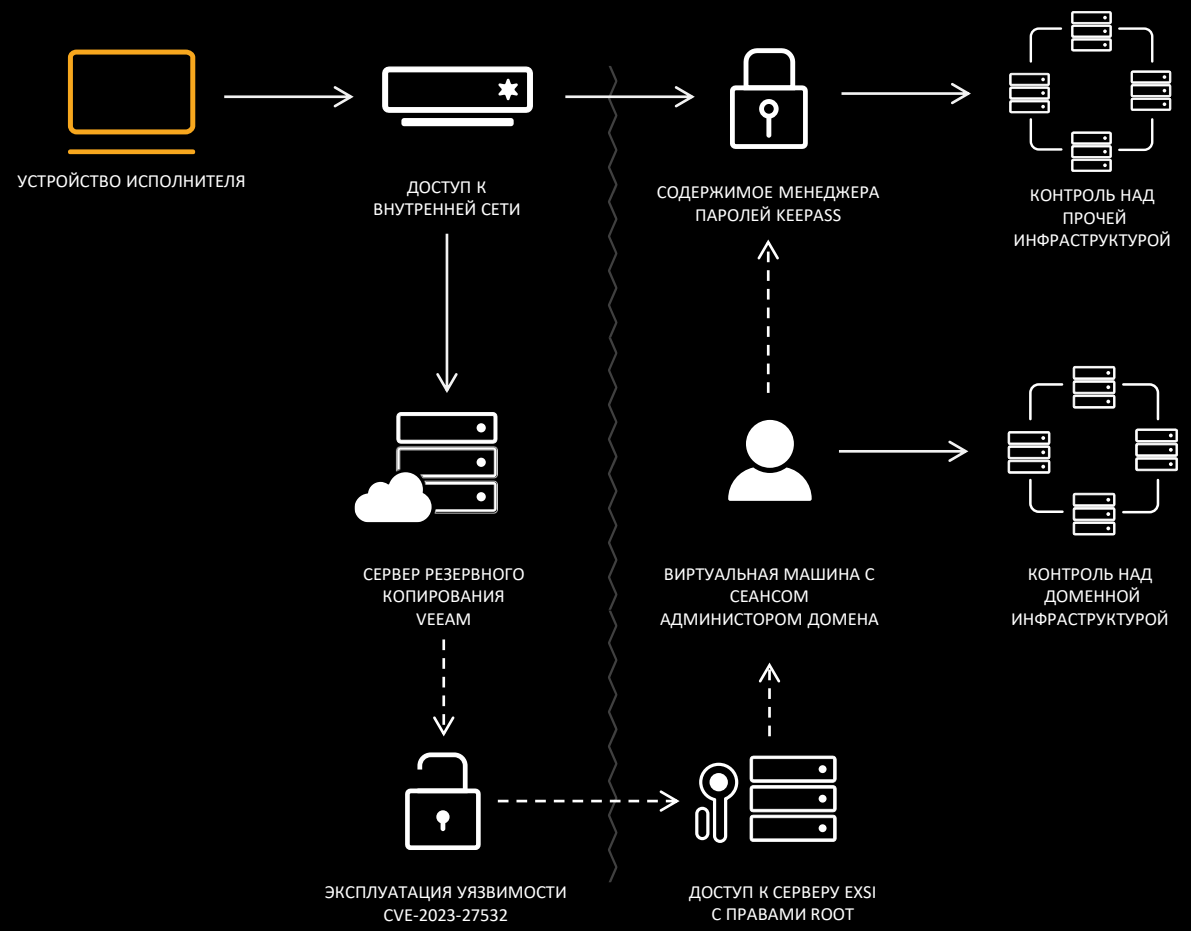
ПРИМЕР: ИСПОЛЬЗОВАНИЕ УЯЗВИМОСТИ VEEAM

МОДЕЛЬ НАРУШИТЕЛЯ: РЯДОВОЙ СОТРУДНИК С МИНИМАЛЬНЫМИ ПРАВАМИ ДОСТУПА

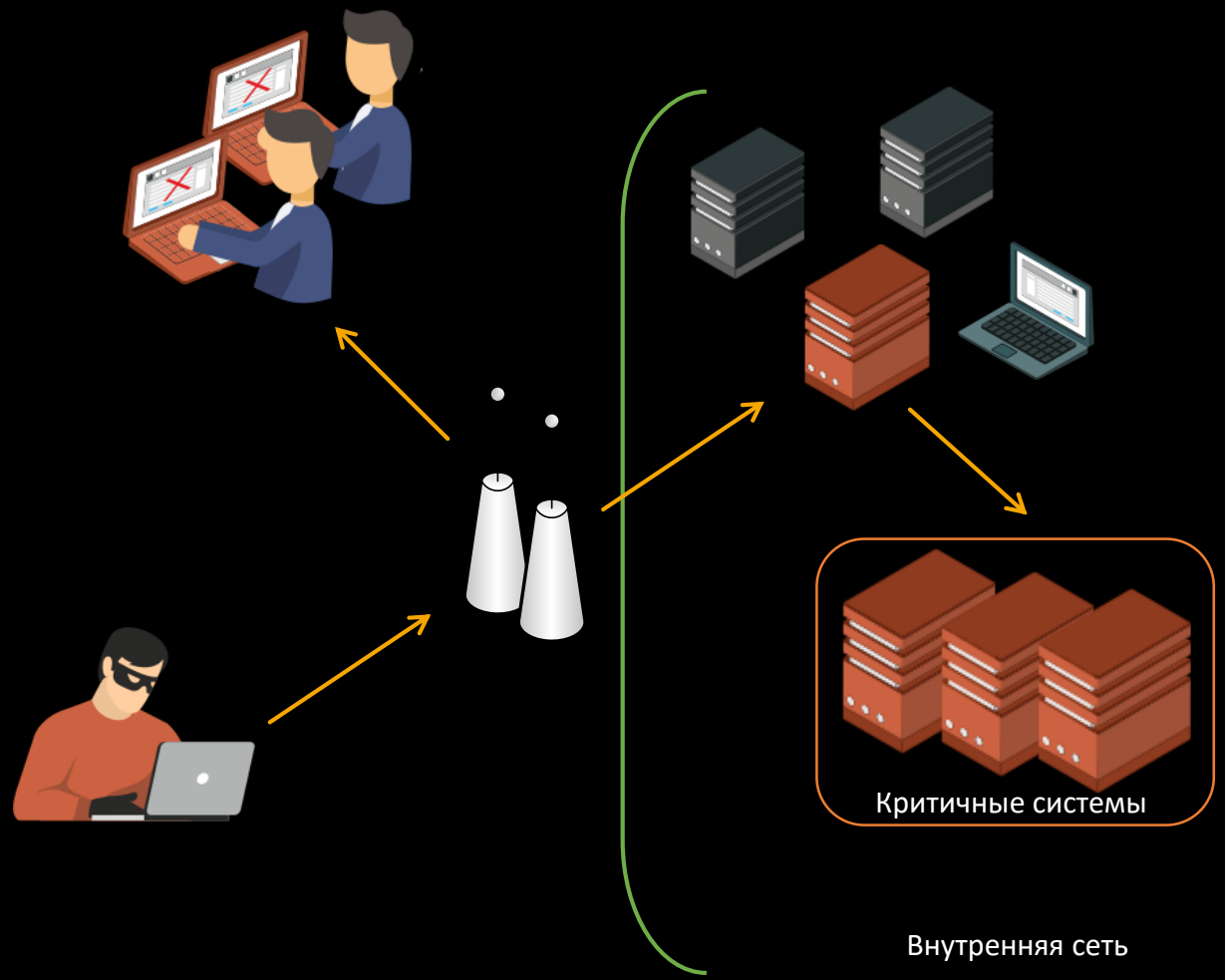
Шаг 1. Во внутренней сети обнаружили сервер резервного копирования Veeam

Шаг 2. После эксплуатации уязвимости получили имя пользователя и пароль для доступа к системе виртуализации ESXI

Шаг 3. Получили доступ к виртуальной машине с незаблокированным сеансом администратора домена. В сеансе обнаружили разблокированный менеджер паролей KeePass



АНАЛИЗ ЗАЩИЩЕННОСТИ БЕСПРОВОДНЫХ СЕТЕЙ



- Проверяются возможности получения доступа к внутренним ресурсам через беспроводные сети
- Работы проводятся очно на объекте
- Проверки выполняются вручную

УЦСБ

АНАЛИЗ ЗАЩИЩЕННОСТИ БЕСПРОВОДНЫХ СЕТЕЙ

Часто встречающиеся проблемы:

- использование словарных паролей
- несанкционированные точки доступа
- уязвимые устройства
- доступ к корпоративной сети из гостевых сетей Wi-Fi
- отсутствие изоляции клиентов
- небезопасная конфигурация сети

Примеры:

- получение доступа к беспроводной сети путем атаки перебора на рукопожатие WPA2-PSK
- компрометация доменных УЗ через WPA2-Enterprise
- получение доступа к корпоративной сети через IP-камеру с беспроводным интерфейсом
- компрометация АРМ через уязвимый адаптер беспроводной мышки

УЦСБ

ПРИМЕР: ДОСТУП К ВНУТРЕННЕЙ СЕТИ ЧЕРЕЗ IP-КАМЕРУ

МОДЕЛЬ НАРУШИТЕЛЯ:
ПОСТОРОННИЙ ВНЕ ОФИСА

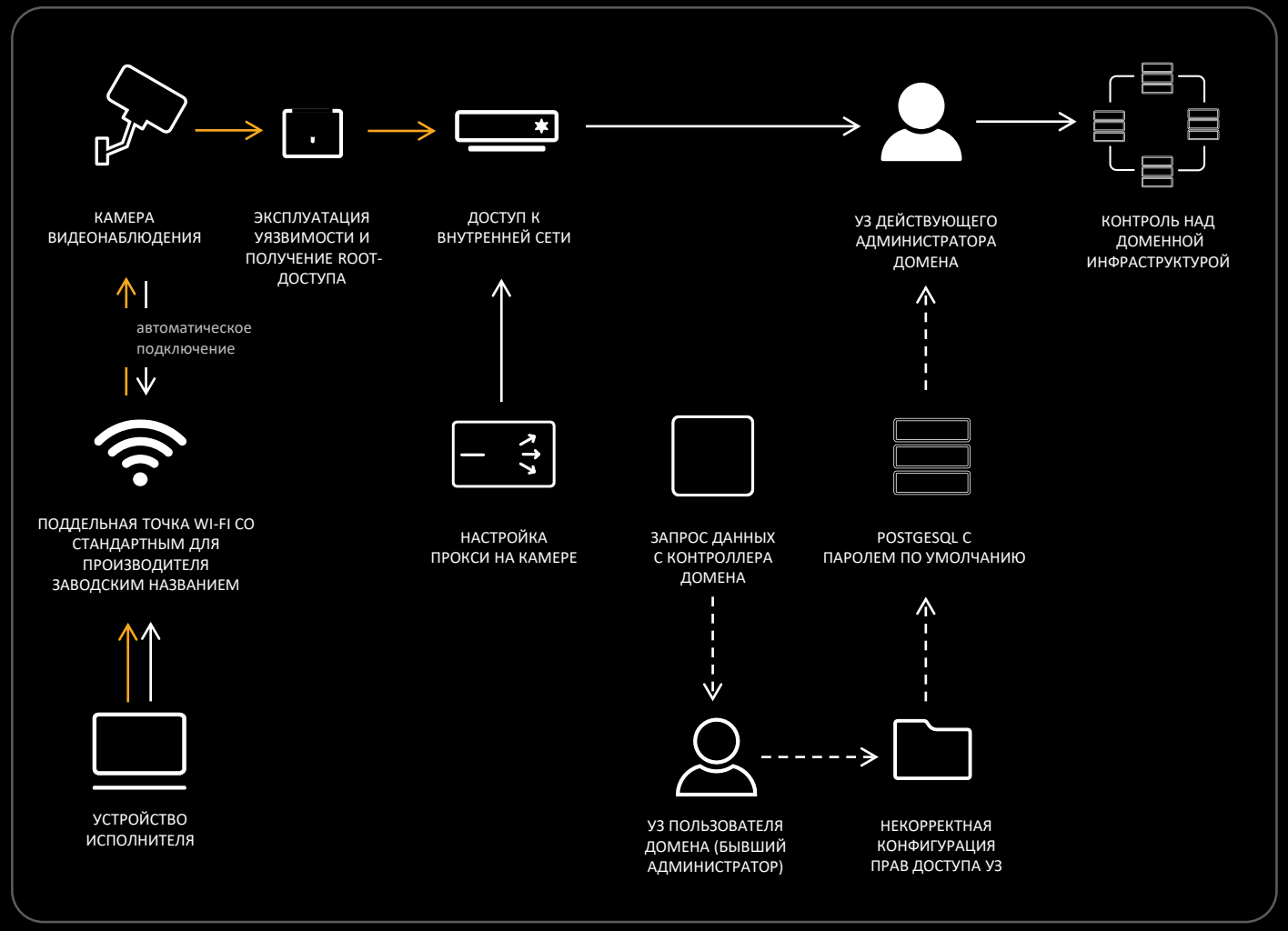
Шаг 1. Обнаружили IP-камеры снаружи объекта. Создали точку доступа со специальным именем, после чего одна из камер автоматически подключилась к этой точке доступа

Шаг 2. Проэксплуатировали уязвимость IP-камеры. Настроили на IP-камере проксирование во внутреннюю сеть

Шаг 3. Во внутренней сети обнаружили БД PostgreSQL с паролем по умолчанию. В БД обнаружили доменную УЗ

Шаг 4. Изучили домен и обнаружили у полученной УЗ право DCsync

Шаг 5. Используя полученную УЗ, выгрузили учетные данные администратора домена



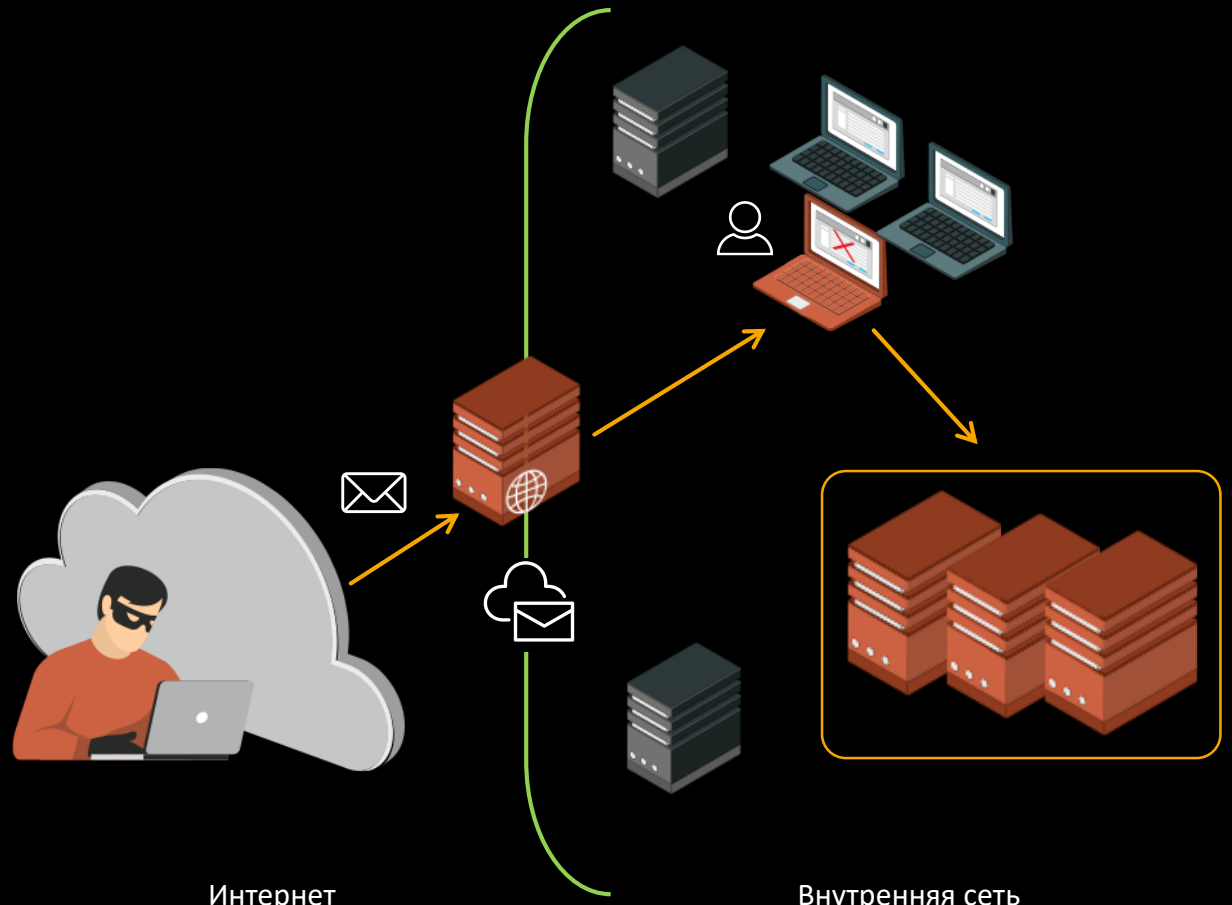
УЦСБ

ОПРОС №2

Проверяете ли вы уровень осведомленности сотрудников в вопросах ИБ?

УЦСБ

ТЕСТИРОВАНИЕ МЕТОДАМИ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ



- Проверяются средства защиты и уровень осведомленности сотрудников
- Работы проводятся удаленно или на объекте

УЦСБ

ТЕСТИРОВАНИЕ МЕТОДАМИ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

Часто встречающиеся проблемы:

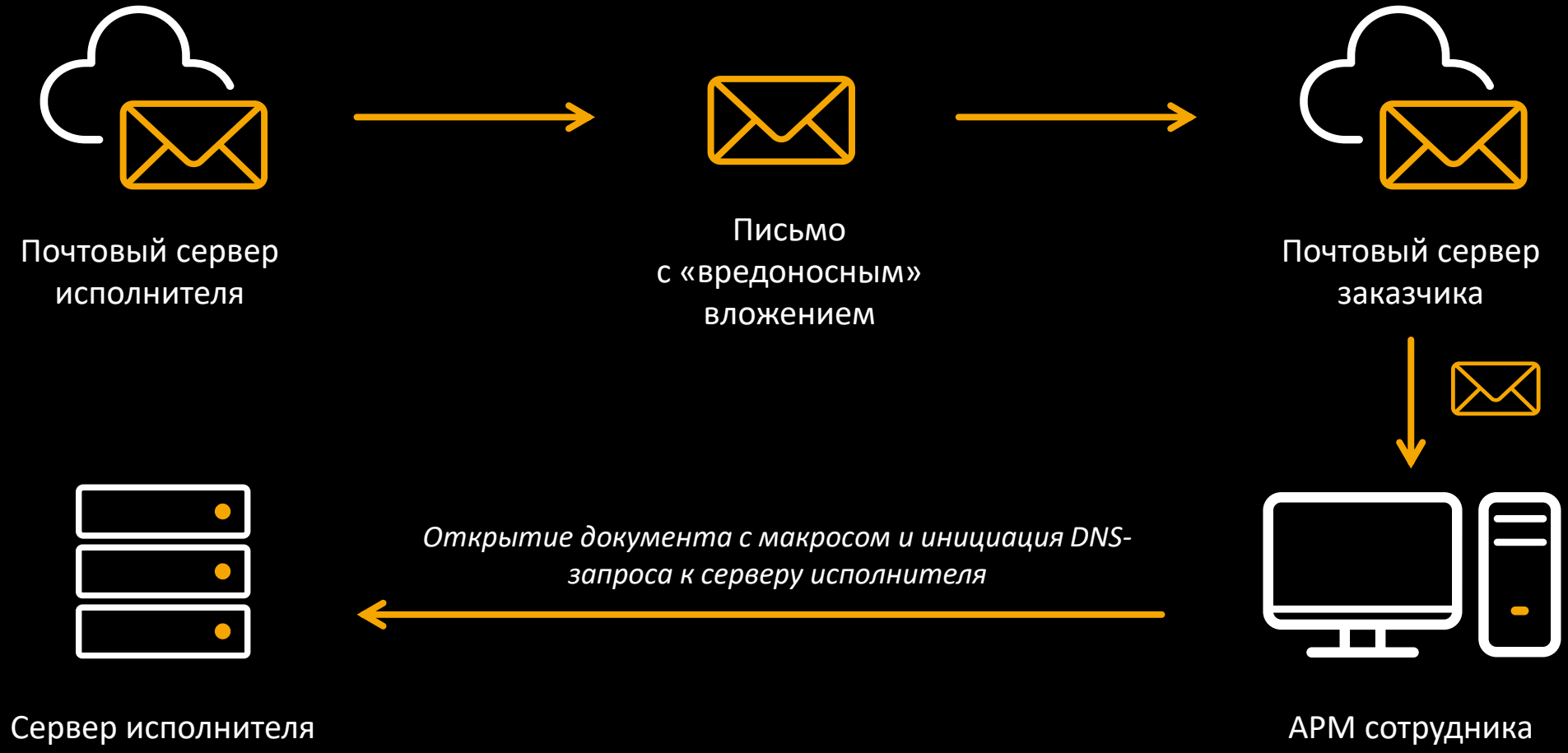
недостатки конфигурации СЗИ

низкий уровень осведомленности сотрудников

Примеры:

- выполнение кода на рабочей станции после открытия вложения из письма
- выполнение кода на рабочей станции после подключения USB-накопителя
- ввод учетных данных на фишинговом сайте после перехода по ссылке из письма

ПРИМЕР: ВЫПОЛНЕНИЕ КОДА НА РАБОЧЕЙ СТАНЦИИ



УЦСБ

ПЕНТЕСТ ОКИИ НА ПРАКТИКЕ

А ВДРУГ ЧТО-ТО СЛОМАЕТСЯ?

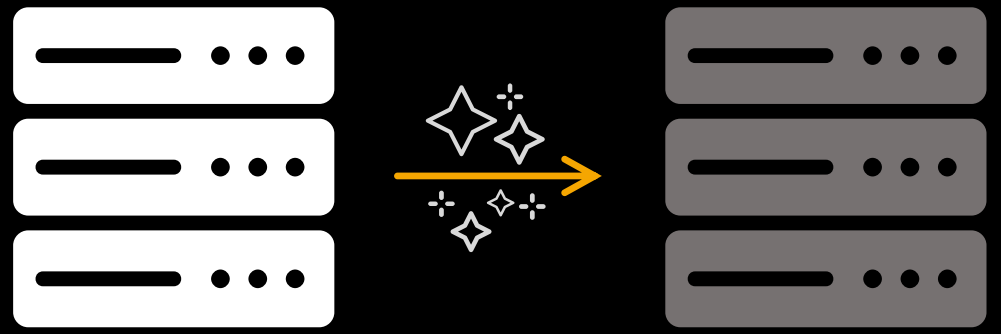
УЦСБ

ЦИФРОВЫЕ ДВОЙНИКИ

aka тестовый контур, тестовый стенд, дубликат, копия

Предотвращаются риски:

- избыточной нагрузки
- избыточной генерации данных
- нежелательных изменений данных или конфигурации
- отказа в обслуживании



КАК СДЕЛАТЬ ПЕНТЕСТ МАКСИМАЛЬНО ЭФФЕКТИВНЫМ?

Перед пентестом:

- выбирайте тот **вид услуг**, который подходит для **ваших целей**
- определите, **какие задачи** вы хотите **решить**
- прописывайте в ТЗ только те **виды работ**, которые **соответствуют вашим задачам**
- выбирайте **надежных подрядчиков**, зарекомендовавших себя на рынке
- постарайтесь решить внутренние вопросы **до проведения работ**

КАК СДЕЛАТЬ ПЕНТЕСТ МАКСИМАЛЬНО ЭФФЕКТИВНЫМ?

Во время пентеста:

- выделите **ответственных сотрудников**, которые будут контактировать с пентестерами
- обеспечьте необходимый для проведения работ **доступ**
- старайтесь **оперативно решать** организационные **вопросы**
- следите за **ходом работ**, но оставляйте для подрядчика **элемент свободы**
- **общайтесь с пентестерами!**

КАК СДЕЛАТЬ ПЕНТЕСТ МАКСИМАЛЬНО ЭФФЕКТИВНЫМ?

После пентеста:

- не стесняйтесь **задавать вопросы** и высказывать **пожелания** при согласовании отчета
- **изучите** предложенные **рекомендации**
- запланируйте **выполнение рекомендаций**, которые считаете подходящими
- проведите **разбор результатов с сотрудниками** ИБ и, при необходимости, с другими сотрудниками
- проведите **контроль** устранения уязвимостей и недостатков

РЕЗЮМЕ

Пентесты позволяют:

- оценить реальный уровень защищенности ресурсов
- проверить возможность реализации НС

На практике пентест ОКИИ:

- проводится с оглядкой на НПА
- учитывает требования к отказоустойчивости
- может состоять из различных видов работ

Нужно обращать внимание на НПА:

- УП 250
- ФЗ 187
- Приказ ФСБ 213
- Постановление Правительства 1272
- Приказ ФСТЭК 239
- Положения ЦБ РФ 683, 757, 821

Пентест будет эффективным при:

- осознанном подходе к ТЗ
- выборе надежного подрядчика
- оперативном решении организационных вопросов
- контроле выполнения полученных рекомендаций

УЦСБ

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	PAM 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
28.08	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?

Дмитрий Зубарев

Старший специалист по анализу защищенности

Прохор Садков

Руководитель направления анализа защищенности

2024

sec@ussc.ru

sec.ussc.ru