ЦЕНТР
КИБЕРБЕЗОПАСНОСТИ

sec.ussc.ru

АНАЛИЗ ЗАЩИЩЕННОСТИ И ПЕНТЕСТЫ

Услуги Центра кибербезопасности УЦСБ

Уральский центр систем безопасности (УЦСБ)

> 16
лет на рынке

> 900
профессионалов в штате

> 1500
завершенных проектов

Топ-100 крупнейших отечественных ИТ-компаний [1]

Топ-15 крупнейших компаний России в сфере защиты информации [2]

Компетенции

- Информационная безопасность
- Информационные технологии
- Инженерно-технические средства охраны
- Анализ защищенности
- Центры обработки данных
- Умный дом
- Сервисный центр

[1] Рейтинг CNews100: Крупнейшие ИТ-компании России 2022
[2] Рейтинг CNews Security: Крупнейшие компании России в сфере защиты информации 2022

Риски

на 20,8%

инцидентов информационной безопасности стало больше за прошедший год

> 15%

всех компьютеров хотя бы раз подвергались веб-атаке с использованием вредоносных программ

12 дней

в среднем проходит с момента возникновения уязвимости до ее эксплуатации

Периметр безопасности размывается

Все больше данных хранится в облачных средах, а удаленная работа стала нормой

Вредоносные инструменты становятся доступнее

Теневой бизнес активно предоставляет вредоносное ПО в качестве услуги, аренда шифровальщиков поставлена на поток

Обеспечивать безопасность иностранного ПО стало сложнее

В ряде случаев больше невозможно устранять уязвимости в продуктах зарубежных разработчиков с помощью регулярных обновлений

Защитите свой бизнес от кибератак

Проверим безопасность вашей ИТ-инфраструктуры, информационных систем и программных продуктов. Выявим возможные векторы атаки и дадим рекомендации, как их предотвратить. Поможем принять меры заблаговременно — до наступления ИБ-события

АНАЛИЗ ЗАЩИЩЕННОСТИ

- внешнего периметра
- внутренней сети
- беспроводных сетей
- логического функционала веб- и мобильных приложений
- от атак типа «отказ в обслуживании» (DoS)
- тестирование методами социальной инженерии

Опыт и экспертиза

7 лет
лет практики

6
зафиксированных уязвимостей нулевого дня

150+
проектов для среднего и крупного бизнеса

15+
квалифицированных специалистов по анализу защищенности (пентестеров)

- Система менеджмента качества по стандартам ISO 9001
- Лицензии ФСБ России (№454 от 05.08.2013) и ФСТЭК России № Л024-00107-00/00580547 от 08.10.2007, № Л050-00107-00/00579687 от 08.10.2007)
- Использование методик на основе международных стандартов и рекомендаций (NIST, OWASP, PCI DSS)
- Команда профессионалов, чья экспертиза подтверждена зарегистрированными уязвимостями, дипломами и сертификатами по кибербезопасности (OSCP, OSWE, OSCE, CISA, CISM, CISSP, CRISC и другие)
- Опыт, изложенный в отраслевых СМИ и профессиональной литературе.

Отраслевой опыт

Финансы и страхование | Госсектор | ИТ и телеком | Энергетика | Металлургия | Нефтегаз | Транспорт | Машиностроение | Сельское хозяйство | Ритейл

Услуги

Анализ защищенности внешнего периметра

Цель: оценить защищенность критических систем и конфиденциальной информации от атак из сети Интернет (внешнее тестирование на проникновение)

Что мы сделаем:

Выполним за 15+ рабочих дней

- Найдем чувствительную информацию в открытых источниках, факты ее утечки
- Выявим уязвимости вручную и с помощью специальных инструментов
- Проведем инвентаризацию ресурсов компании, доступных из Интернета
- Найдем возможные сценарии проникновения во внутреннюю сеть
- Подготовим рекомендации для устранения найденных уязвимостей и повышения общей защищенности ИТ-инфраструктуры

Услуга не включает проверку логического функционала веб-приложений

Анализ защищенности внутренней сети

Цель: оценить защищенность критических систем и конфиденциальной информации от атак из корпоративной сети (внутренние тестирование на проникновение)

Что мы сделаем:

Выполним за 15+ рабочих дней

- Найдем уязвимости во внутренних службах и сервисах компании
- Выясним насколько безопасен удаленный доступ к ним
- Проверим внутренние контроли безопасности и корректность настройки сетевых сервисов
- Определим возможности получения несанкционированного доступа к чувствительной информации
- Определим избыточные права доступа к данным
- Подготовим рекомендации для устранения найденных уязвимостей и повышения общей защищенности ИТ-инфраструктуры

При необходимости проведем проверку беспроводных сетей

Анализ защищенности беспроводных сетей

Цель: оценить риски проникновения через беспроводные сети компании и проверить защищенность их пользователей

Что мы сделаем:

Выполним за 15+ рабочих дней

- Идентифицируем вероятные векторы кибератаки через Wi-Fi и радиоканал беспроводных устройств
- Проверим защищенность и сегментацию беспроводных сетей компании
- Найдем неучтенные точки доступа к сетевой инфраструктуре
- Проверим возможность перехвата учетных данных пользователей беспроводных сетей

Анализ защищенности логического функционала мобильных и веб-приложений

Цель: оценить защищенность приложения от атак со стороны пользователей

Что мы сделаем:

Выполним за 10+ рабочих дней

- Проанализируем бизнес-логику приложения на наличие ошибок
- Исследуем клиентскую (front-end) и серверную (back-end) части приложения на баги и некорректную конфигурацию
- Выявим уязвимости, допущенные при разработке приложения

По запросу проанализируем исходный кода вашего приложения методом (SAST, DAST)

Тестирование методами социальной инженерии

Цель: оценить уровень информированности сотрудников о базовых правилах кибербезопасности

Сценарии тестирования:

Выполним за 10+ рабочих дней

- Через электронную почту: отправка «вредоносного» файла во вложении или ссылки на фишинговый ресурс (сайт, внутренний сервис, мобильное приложение)
- Через подброс «вредоносных» носителей
- Через «вредоносный» QR-код
- Другие форматы (обсуждается индивидуально)

Методы комплексно дополняют внутреннее и внешнее тестирование на проникновение

1 из 3 Каждый третий сотрудник рискует запустить вредоносный код на рабочем компьютере

1 из 5 Каждый пятый вводит учетные данные в поддельную форму аутентификации

По статистике проектов Центра кибербезопасности УЦСБ

Анализ защищенности от атак типа «отказ в обслуживании»

Цель: оценить устойчивость ИТ-инфраструктуры к DoS-атакам прикладного уровня (L7-атаки)

Что мы сделаем:

Выполним за 15+ рабочих дней

Смоделируем атаки на исчерпание ресурсов приложения:

- запросы на аутентификацию
- GET-запросы к страницам приложения
- запросы с длинными строками

Воспроизведем атаки Slow HTTP*:

- Slowloris
- Slow HTTP POST
- Slow Read

Подготовим рекомендации для устранения найденных уязвимостей и повышения общей защищенности ИТ-инфраструктуры

*Атака на веб-сервисы, направленная на замедление или полное прекращение обработки запросов пользователей

Как анализ защищенности поможет вашему бизнесу?

Вы получите детальный отчет о состоянии защищенности ИТ-инфраструктуры компании,
оценку рисков для кибербезопасности и четкий план действий по устранению уязвимостей

Даст возможность действовать на опережение и снизить возможные риски

Вовремя обнаруженные и исправленные уязвимости помогут существенно снизить риск успешной кибератаки, минимизировать возможный финансовый и репутационный ущерб для компании

Поможет оценить эффективность используемых мер защиты

Независимый анализ состояния вашей инфраструктуры подсветит ее «тонкие места», даст возможность объективно оценить, эффективны ли ваши механизмы защиты

Позволит соответствовать отраслевым нормативам и внутренним стандартам

Проверка защищенности инфраструктуры позволит привести ее в соответствие требованиям регуляторов — например, приказов ФСТЭК России № 239 № 21, № 17, положениям Банка России № 683-П, 719-П, 757-П, ГОСТ 57580, указа Президента Российской Федерации № 250

Преимущества работы с Центром кибербезопасности УЦСБ

Проектное управление
Над решением вашей задачи будет работать целая команда. Четкое распределение зон ответственности и ролей поможет обеспечить сдачу проекта в срок с результатами, отвечающими вашим ожиданиям или даже выше

Гибкость и фокусный подход
Мы не работаем по шаблону, а отталкиваемся от вашей специфики и потребностей, формируя состав услуг индивидуально. Качество нашей работы определяет ее польза для вашего бизнеса

Все компетенции и инструменты в одном месте

Центр кибербезопасности УЦСБ объединяет исчерпывающий комплекс инструментов и услуг в области ИБ. Какая бы потребность не возникла у вас завтра, мы всегда сможем предложить для нее адекватное решение

Схемы выполненных атак

Схемы выполненных атак: сценарий №1

МОДЕЛЬ НАРУШИТЕЛЯ: ГОСТЬ В ОФИСЕ

Шаг 1. Нашли доменный ноутбук в переговорке со свободным доступом для посетителей, который подключен к закрытой гостевой сети Wi-Fi и к проводной рабочей сети с доменом

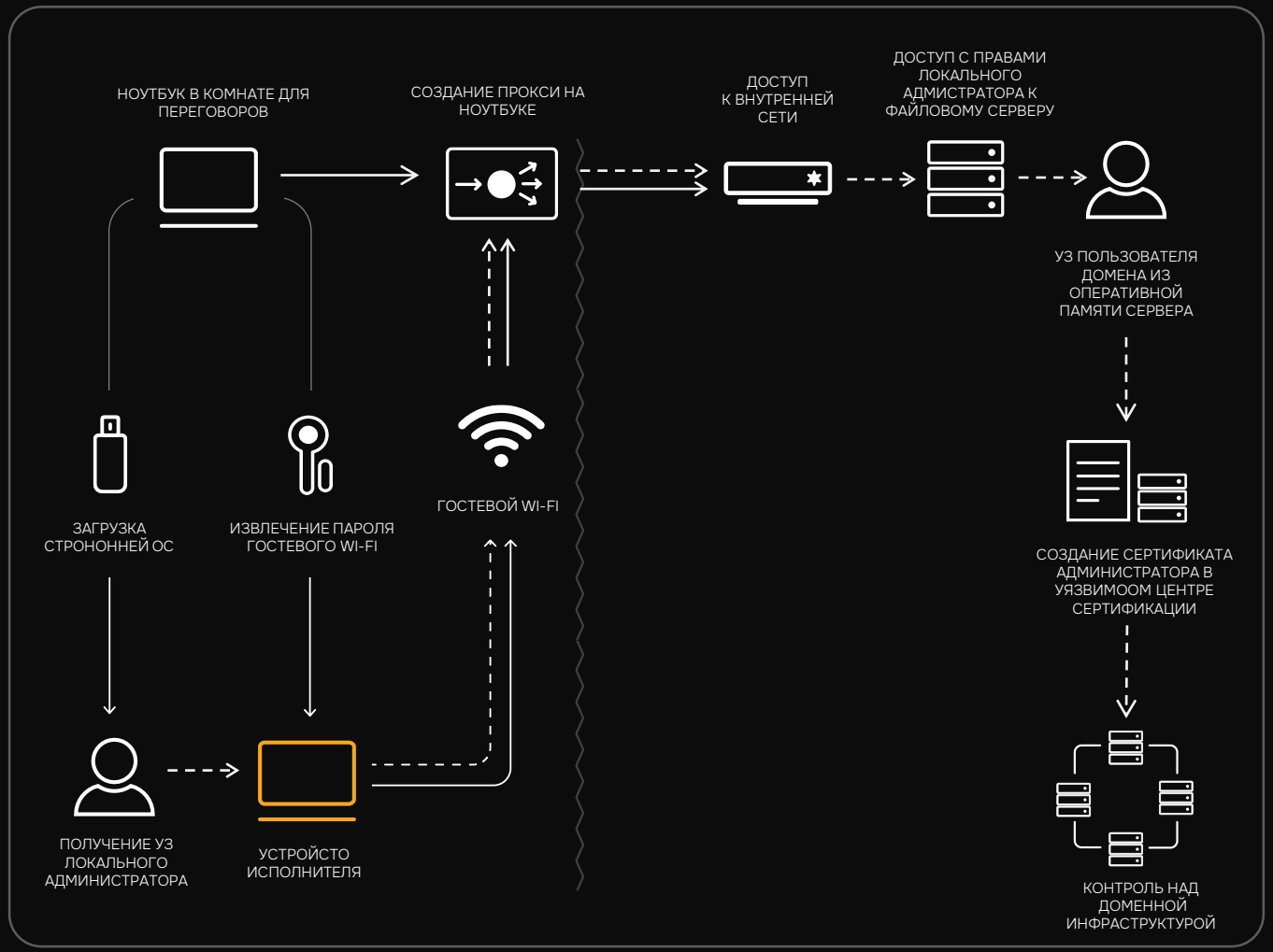
Шаг 2. Загрузили ноутбук с загрузочного USB и извлекли хэш локального администратора

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

Шаг 4. Хэш локального администратора ноутбука позволил получить доступ к файловому серверу с правами локального администратора. Из памяти файлового сервера извлекли логин и пароль доменного пользователя

Шаг 5. Используя учетную запись доменного пользователя, воспользовались уязвимостью центра сертификации AD и выпустили сертификат от имени доменного администратора

Шаг 6. С помощью сертификата доменного администратора получили доступ ко всем устройствам в доменной сети заказчика



Схемы выполненных атак: сценарий №2

МОДЕЛЬ НАРУШИТЕЛЯ: ГОСТЬ В ОФИСЕ

Шаг 1. Обошли port security, подключились к сети принтеров и получили доменную учетную запись одного из многофункциональных устройств, которая использовалась для связи с LDAP

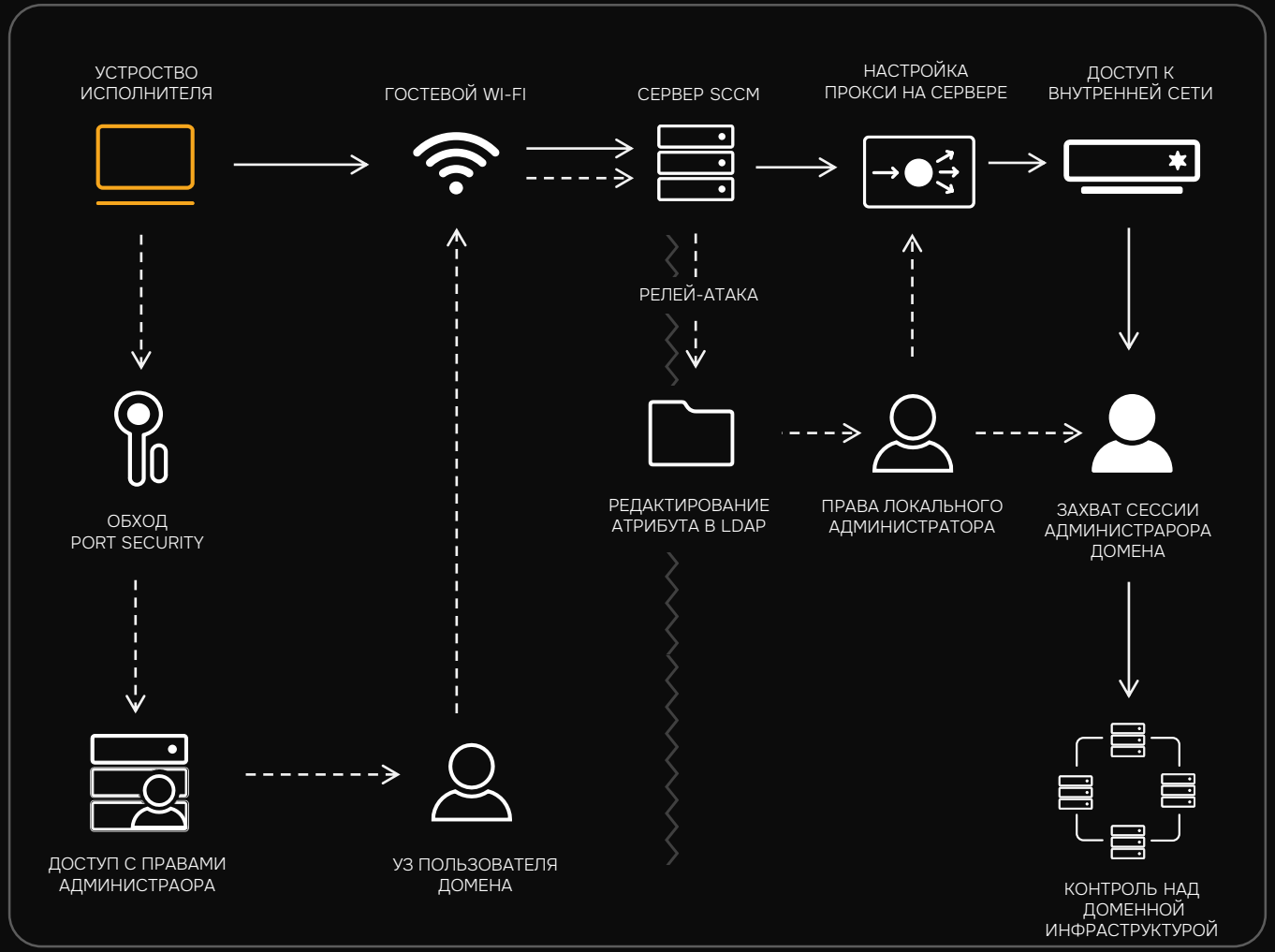
Шаг 2. Подключились к гостевой сети Wi-Fi и обнаружили доступность сервера SCCM и службы LDAP контроллера домена из этой сети

Шаг 3. Провели релей-атаку и получили доступ к LDAP от имени сервера SCCM

Шаг 4. Изменили атрибут учетной записи сервера SCCM и получили доступ к нему с правами локального администратора

Шаг 5. Захватили сессию доменного администратора на сервере SCCM

Шаг 6. С контроллера домена получили аутентификационные данные других администраторов домена



Схемы выполненных атак: сценарий №3

МОДЕЛЬ НАРУШИТЕЛЯ: ПОСТОРОННИЙ ВНЕ ОФИСА

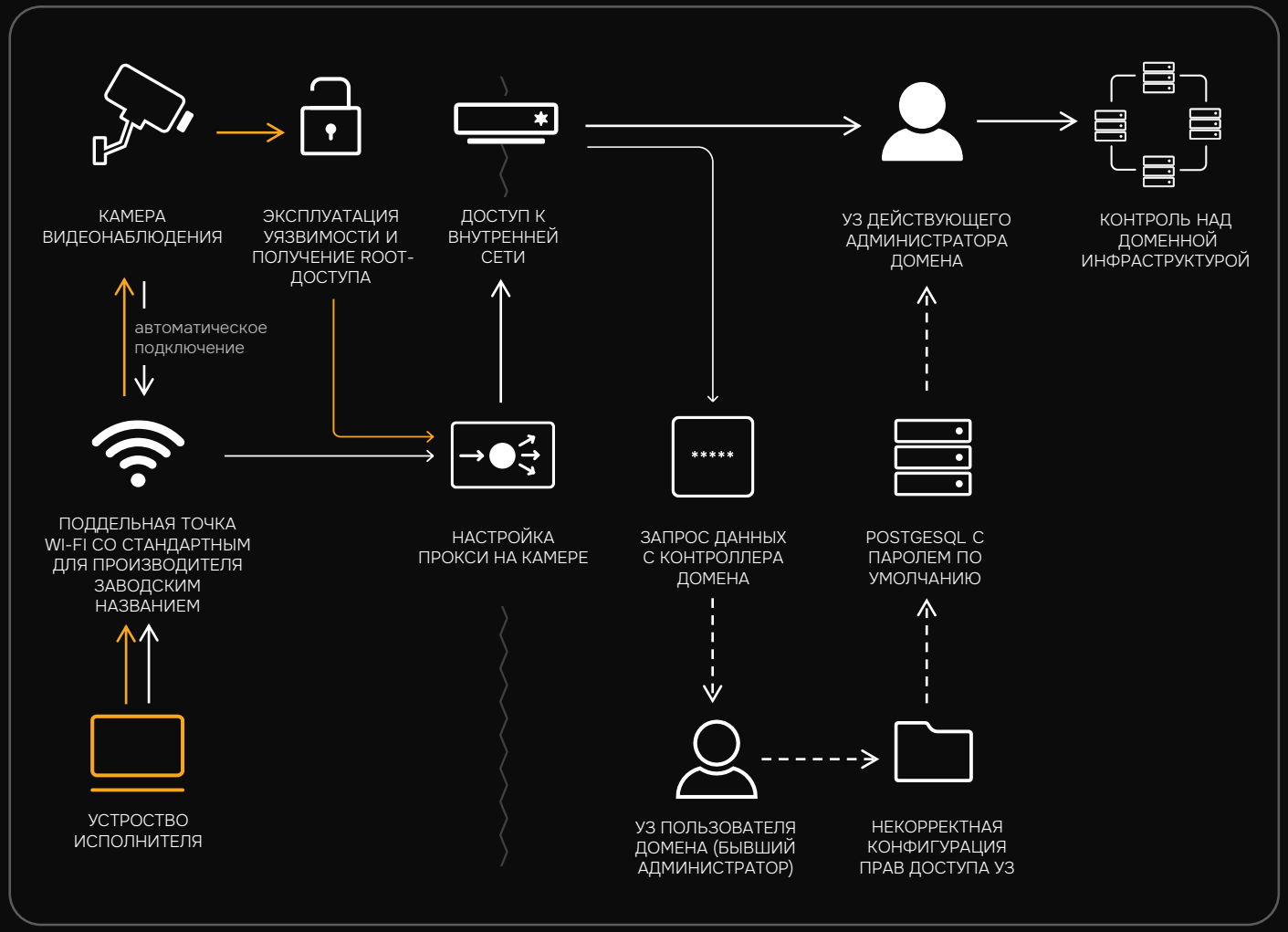
Шаг 1. Обнаружили использование наружных камер видеонаблюдения у заказчика, находясь на улице. Создали открытую точку доступа с заводским именем от производителя, после чего одна из камера автоматически подключилась к этой точке доступа

Шаг 2. Поскольку камера оказалась уязвима к удаленному выполнению кода, получили доступ к ней по SSH, а уже через него «прокинули» доступ во внутреннюю сеть заказчика

Шаг 3. Во внутренней сети обнаружили базу Postgresql данных с паролями по умолчанию. Внутри базы данных нашли учетную запись пользователя домена

Шаг 4. При помощи учетной записи смогли прочитать конфигурацию AD и выяснить, что у этой учетной записи есть право на DCsync – получение с контроллеров домена аутентификационных данных других пользователей. Возможно, ранее учетная запись принадлежала администратору или права доступа были выданы ошибочно

Шаг 5. Получили аутентификационные данные действующего администратора домена



Схемы выполненных атак: сценарий №4

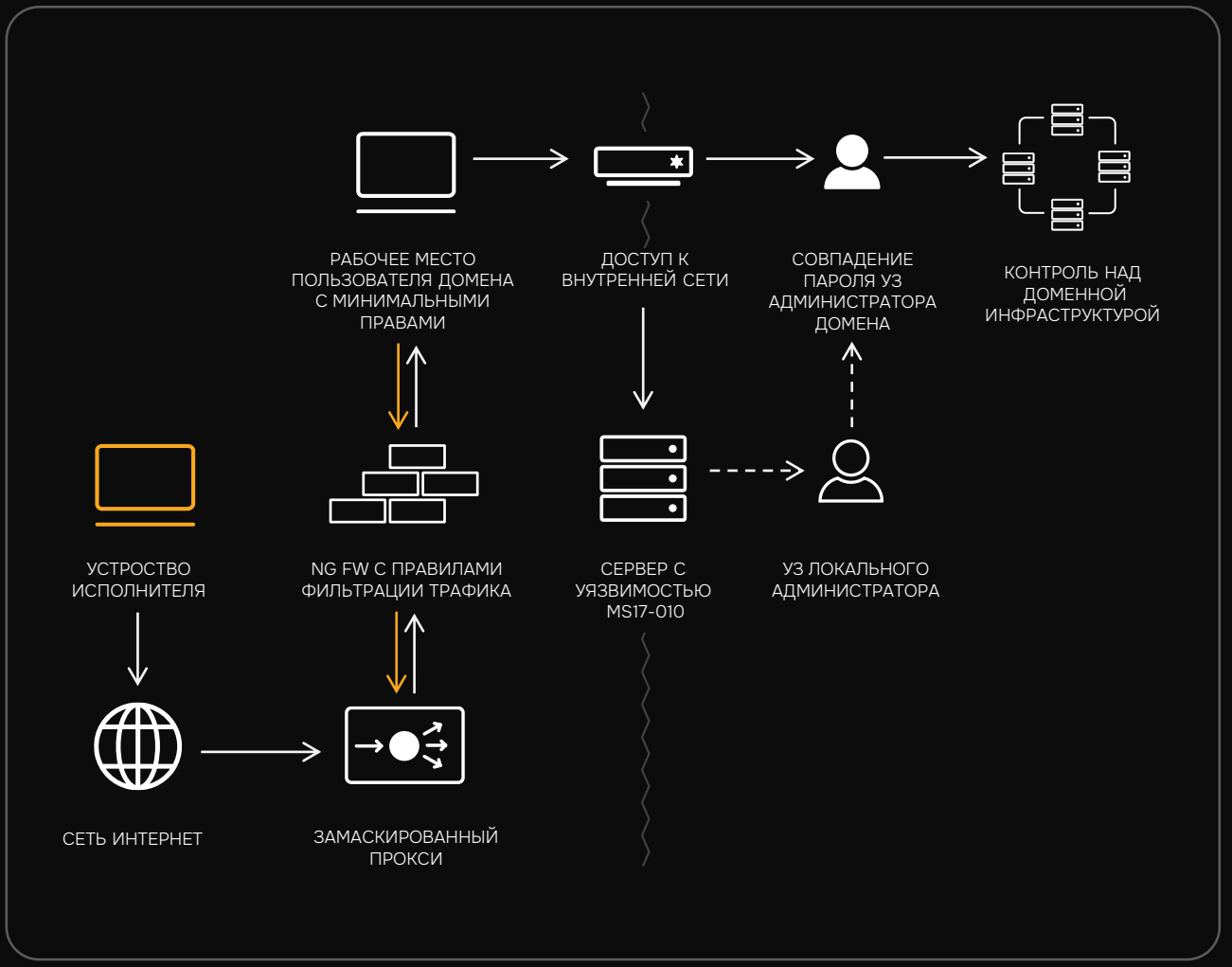
МОДЕЛЬ НАРУШИТЕЛЯ: СОТРУДНИК КОМПАНИИ С МИНИМАЛЬНЫМИ ПРАВАМИ И ОГРАНИЧЕННЫМ ДОСТУПОМ В ИНТЕРНЕТ

Шаг 1. Обошли правила фильтрации файрволла и настроили замаскированный прокси-доступ из Интернета к внутренней сети. При настройке исключили возможность подключения третьих лиц к организованному доступу

Шаг 2. Через Интернет и настроенный доступ подключили атакующую ОС к внутренней сети заказчика

Шаг 3. В результате сканирования во внутренней сети обнаружили уязвимость MS17-010 на рабочей станции

Шаг 4. В результате эксплуатации уязвимости получили логин и пароль локального администратора. Пароль локального администратора совпал с паролем доменного



Схемы выполненных атак: сценарий №5

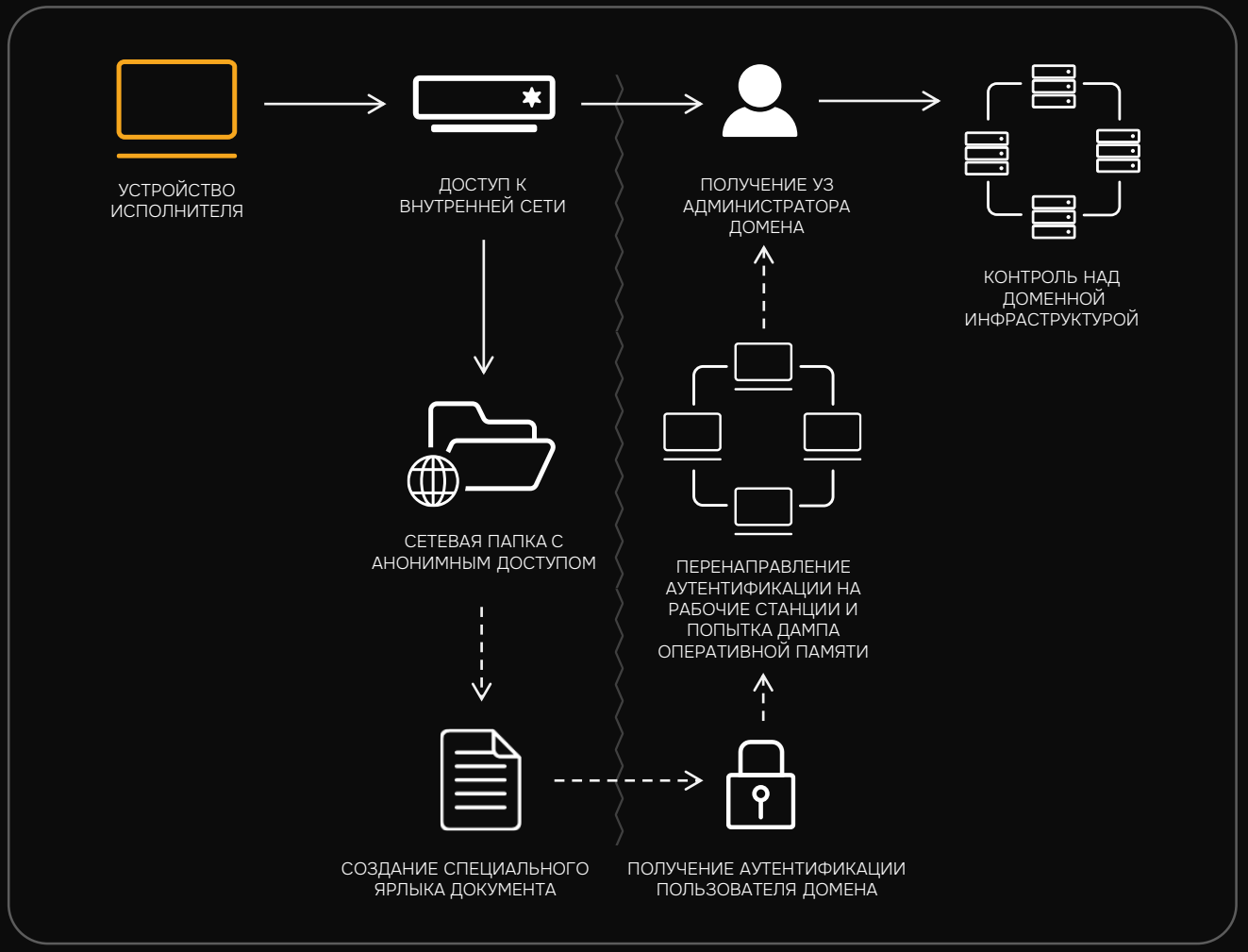
МОДЕЛЬ НАРУШИТЕЛЯ: РЯДОВОЙ СОТРУДНИК С МИНИМАЛЬНЫМИ ПРАВАМИ ДОСТУПА

Шаг 1. Закинули специальный ярлык на сетевую шару

Шаг 2. Получили входящую аутентификацию от одного из пользователей

Шаг 3. Перенаправили аутентификацию на другие устройства в домене и получили командную строку от имени этого пользователя. Любопытная деталь: пользователь оказался администратором домена

Шаг 4. Сняли несколько дампов оперативной памяти, в итоге из одного из них получили логин и пароль другого доменного администратора



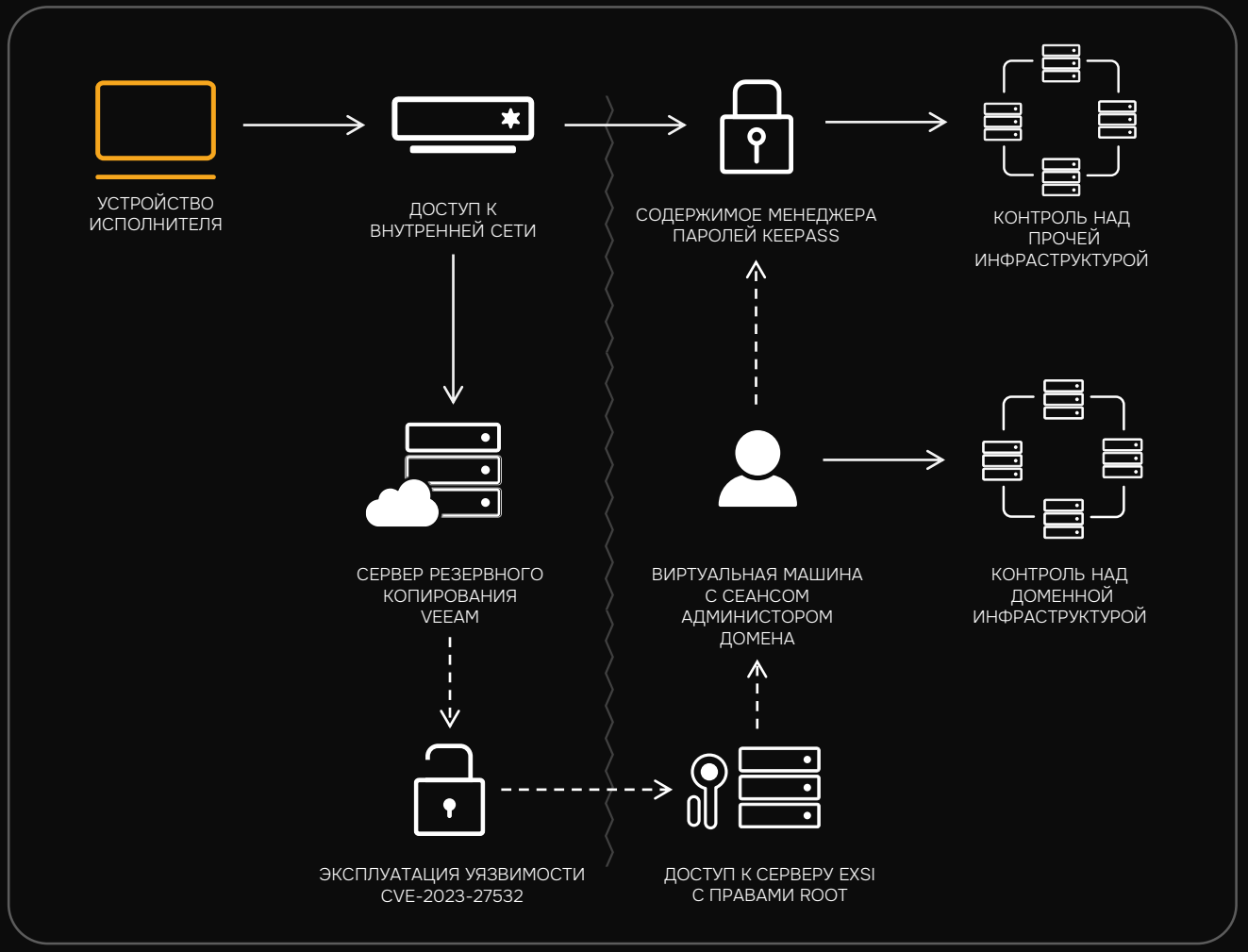
Схемы выполненных атак: сценарий №6

МОДЕЛЬ НАРУШИТЕЛЯ: РЯДОВОЙ СОТРУДНИК С МИНИМАЛЬНЫМИ ПРАВАМИ ДОСТУПА

Шаг 1. По внутренней сети обнаружили сервер резервного копирования Veeam

Шаг 2. После эксплуатации уязвимости получили логин и пароль для системы виртуализации ESXI

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



ЦЕНТР КИБЕРБЕЗОПАСНОСТИ

sec.ussc.ru

cybersec@ussc.ru