

**Учебный центр ООО «Скилфэктори»**

совместно с

**Федеральное государственное автономное**

**образовательное учреждение высшего образования**

**Национальный исследовательский ядерный университет «МИФИ».**

Выпускная квалификационная работа

на тему:

**“Метод и система сбора поверхности атаки для внешнего периметра  
организации”**

Программа дополнительного профессионального образования

“Информационная безопасность”

**Выполнил студент МИФИВ**

**3 поток:**

Евгений Костенко

**Научный руководитель:**

Александр Цуканов

Москва, 2024

## ОГЛАВЛЕНИЕ

Глава	Содержание	Стр.
	ВВЕДЕНИЕ	5
ГЛАВА 1	ВВЕДЕНИЕ В СБОРА ПОВЕРХНОСТИ АТАКИ ДЛЯ ВНЕШНЕГО ПЕРИМЕТРА ОРГАНИЗАЦИИ	6
1.1	Что такое поверхность атаки	
1.2	Что такое внешний периметр	
1.3	Основные задачи сбора поверхности атаки	
1.4	Подход к безопасности с позиции атакующего	
1.5	Общие выводы	
ГЛАВА 2	КАРТОГРАФИЯ УЯЗВИМОСТИ: ВЕКТОРЫ АТАК И ПОВЕРХНОСТИ АТАКИ	9
2.1	Векторы атак и поверхностей атаки	
2.2	Распространенные виды векторов атак	
2.3	Цифровые поверхности атак	
2.4	Физические поверхности атак	
2.5	Способы защиты от векторов атак	
ГЛАВА 3	СТРАТЕГИИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ: АНАЛИЗ И УПРАВЛЕНИЕ ПОВЕРХНОСТЬЮ АТАКИ	17

3.1	Анализ и мониторинг поверхности атаки	
3.2	Минимизация цифровой поверхности атаки	
3.3	Минимизация физической поверхности атаки	
3.4	Способ помочь сократить физическую поверхность атак	
3.5	Снижение и управление поверхностью атаки	
ГЛАВА 4	АРХИТЕКТУРА БЕЗОПАСНОСТИ: УПРАВЛЕНИЕ И ОПТИМИЗАЦИЯ ПОВЕРХНОСТИ АТАКИ	24
4.1	Управление поверхностью атаки	
4.2	Инструменты управления поверхностью атаки	
4.3	Метод и система сбора поверхностью атаки	
4.4	Программа управления поверхностью атаки	
ГЛАВА 5	РИСК ОЦЕНКА ПОВЕРХНОСТИ АТАКИ ПОСЛЕ ВЫЯВЛЕНИЯ УЯЗВИМОСТИ	31
5.1	Методология управления рисками	
5.2	Методологии оценки рисков NIST	
5.3	Применение стандарта CVSS	
5.4	Практический анализ уязвимости на основе развернутого практического стенда и результата анализа поверхности	

5.5	Разработка стратегии управления рисками на основе риска аппетита компании и оценки риска ИТ инфраструктуры	
ГЛАВА 6	ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ МЕТОДА И СИСТЕМЫ СБОРА ПОВЕРХНОСТИ АТАКИ ДЛЯ ВНЕШНЕГО ПЕРИМЕТРА ОРГАНИЗАЦИИ	39
6.1	Вариант практической реализации применения метода и системы сбора поверхности атаки для внешнего периметра организации	
6.2	Идентификация и картирование поверхности атаки	
6.3	Измерение и оценка поверхности атаки	
	ЗАКЛЮЧЕНИЕ	47
	СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ	48
	Приложение: Код программы на языке Python	49

## **ВВЕДЕНИЕ**

В современном мире информационных технологий, увеличение числа кибератак требует от организаций активной работы по защите своих информационных ресурсов. Одним из ключевых аспектов обеспечения кибербезопасности является понимание и управление поверхностью атаки. В данной работе мы обсудим, что такое поверхность атаки и внешний периметр, а также разработаем метод и систему сбора информации о поверхности атаки для внешнего периметра организации.

# ГЛАВА 1

## ВВЕДЕНИЕ В СБОРА ПОВЕРХНОСТИ АТАКИ ДЛЯ ВНЕШНЕГО ПЕРИМЕТРА ОРГАНИЗАЦИИ

### 1.1 Что такое поверхность атаки

**Поверхность атаки (Attack Surface)** — это совокупность уязвимостей, путей и методов, иногда называемых векторами атаки, которые хакеры могут использовать для получения несанкционированного доступа к сети или конфиденциальным данным, а также для осуществления кибератаки. Это могут быть как программные и аппаратные компоненты, так и конфигурационные ошибки или человеческий фактор. Понимание поверхности атаки необходимо для оценки рисков и разработки стратегий защиты. Опционально можно разделить поверхность атаки на три под поверхности: Цифровая поверхность атаки (Digital attack surface), физическая поверхность атаки (Physical attack surface) и поверхность атаки с помощью социальной инженерии (Social engineering attack surface).

### 1.2 Что такое внешний периметр

**Внешний периметр** организации описывает все внешние интерфейсы, через которые организация взаимодействует с внешним миром. Это может включать веб-сайты, публичные API, удаленные доступы и другие интернет-выходы. Внешний периметр часто является первой линией защиты и первой целью для кибератак.

### **1.3 Основные задачи сбора поверхности атаки**

**Возможные примеры использования системы сбора поверхности атаки для внешнего периметра:**

1. Проактивное обнаружение уязвимостей: система может автоматически сканировать внешний периметр на предмет новых или известных уязвимостей, предоставляя команде безопасности возможность устранять их до того, как они будут использованы злоумышленниками.
2. Контроль изменений в конфигурации: мониторинг изменений в конфигурации внешних сервисов помогает обнаружить неавторизованные или подозрительные изменения, которые могут повлиять на безопасность.
3. Оценка рисков и соответствия нормативным требованиям: регулярный анализ и оценка внешнего периметра позволяют организациям оценивать свои риски и поддерживать соответствие требованиям по кибербезопасности, таким как GDPR или HIPAA.

В следующих разделах мы подробнее рассмотрим методы и системы, используемые для сбора и анализа информации о поверхности атаки, приведем примеры реализации таких систем и обсудим лучшие практики и рекомендации по их применению.

## **1.4 Подход к безопасности с позиции атакующего**

Большинство кибератак начинаются с сетевого периметра не случайно.

- В своих атаках злоумышленники не привязаны к списку активов и официальной отсканированной и защищенной сетевым экраном инфраструктуре организации.
- Проводя разведку, атакующие понимают, что основные домены и ключевая инфраструктура будут защищены. Для того чтобы получить доступ, они ищут слабые и упущенные из виду элементы ИТ.
- Простые ошибки в конфигурации на забытом ИТ-элементе становятся началом атак, которые быстро приводят к катастрофическим последствиям.

## **1.5 Общие выводы**

Поверхность атаки включает все потенциальные уязвимости и точки входа, которые могут использовать злоумышленники, и делится на цифровые и физические компоненты, требуя регулярной оценки и смягчения рисков для минимизации киберугроз.

Проактивное управление внешней поверхностью атаки включает непрерывный мониторинг, устранение уязвимостей, применение надежных мер безопасности, таких как межсетевые экраны и системы обнаружения вторжений, а также использование центров мониторинга безопасности (SOC) для обнаружения и реагирования на угрозы в режиме реального времени.



## ГЛАВА 2

# КАРТОГРАФИЯ УЯЗВИМОСТИ: ВЕКТОРЫ АТАК И ПОВЕРХНОСТИ АТАКИ

### 2.1 Векторы атак и поверхностей атаки

**Вектор атаки** — это путь, уязвимость или метод, который злоумышленники могут использовать для доступа к цифровой цели, такой как сеть, система или база данных. Злоумышленники применяют векторы атак, чтобы получить несанкционированный доступ к цифровым целям и дополнительные права.

**Поверхность атаки состоит из всех потенциальных векторов атак.** Большая поверхность атаки включает больше возможных векторов атак.

Векторы атак позволяют злоумышленникам потенциально взломать цель и получить доступ к конфиденциальной информации. Они используют векторы атак для различных целей, например, распространения вредоносного ПО или программ-вымогателей. Организации подвержены воздействию многих векторов атак, представляющих потенциальные проблемы безопасности, но часто многие из них не видны, оставляя организацию уязвимой для атак.

Поверхность атаки включает все потенциальные точки, где злоумышленник может использовать слабые места в системе или сети. Поверхности атак можно разделить на две основные категории: **цифровые и физические.**

Для систематизации подходов к анализу векторов атак и поверхностей атаки можно эффективно использовать матрицу MITRE ATT&CK. Этот глобальный навигационный инструмент предоставляет комплексное

описание тактик и техник, используемых злоумышленниками в процессе кибератак. Включение матрицы в стратегию кибербезопасности позволяет организациям лучше понимать угрозы и уязвимости, а также систематизировать информацию о возможных нападениях.

positive technologies

Решения Продукты Сервисы Ru **БЕСПЛАТНЫЙ ПИЛОТ**

Все продукты: 4 ☐ PT NAD ☐ MaxPatrol SIEM ☐ MaxPatrol EDR ☐ PT Sandbox

☐ Только покрытые техники ☒ Покрытие 77.41%

■ Полное покрытие техники ■ Частичное покрытие техники ■ Требуется эксперт

Разведка	Подготовка ресурсов	Первоначальный доступ	Выполнение	Закрепление	Повышение привилегий	Предотвращение обнаружения	Получение учетных данных
T1589 Сбор информации об атакуемых пользователях (1/3)	T1583 Приобретение инфраструктуры (1/8)	T1078 Существующие учетные записи (4/4)	T1047 Инструментарий управления Windows (2/5)	T1037 Сценарии инициализации при загрузке или входе в систему (2/5)	T1037 Сценарии инициализации при загрузке или входе в систему (2/5)	T1006 Прямой доступ к тому (1/1)	T1003 Получение дампа данных (8/8)
T1590 Сбор информации об атакуемой сетевой инфраструктуре (3/8)	T1584 Компрометация сторонней инфраструктуры (7/7)	T1091 Распространение через съемные носители (5/5)	T1053 Запланированная задача (задание) (5/5)	T1053 Запланированная задача (задание) (5/5)	T1053 Запланированная задача (задание) (5/5)	T1027 Обфусцированные файлы или данные (8/1)	T1040 Прослушивание сетевого трафика (1/1)
T1591 Сбор бизнес-информации об атакуемой организации (1/4)	T1585 Создание учетных записей (1/4)	T1133 Внешние службы удаленного доступа (1/1)	T1059 Интерпретаторы командной строки и сценариев (7/9)	T1078 Существующие учетные записи (4/4)	T1055 Внесение кода в процессы (10/12)	T1036 Маскировка (7/8)	T1056 Перехват ввода/вывода (4/4)
T1592 Сбор информации об атакуемых узлах (4/4)	T1586 Компрометация учетных записей (1/4)	T1190 Недостатки в общедоступном приложении (1/1)	T1072 Средства развертывания ПО (1/1)	T1098 Манипуляции с учетной записью (5/5)	T1068 Эксплуатация уязвимостей для повышения привилегий (10/12)	T1055 Внесение кода в процессы (10/12)	T1100 Метод перебора (4/4)
T1593 Поиск на общедоступных сайтах (1/1)	T1587 Разработка собственных средств (1/4)	T1195 Компрометация цепочки поставок (2/3)	T1129 Общие модули (1/1)	T1133 Внешние службы удаленного доступа (1/1)	T1078 Существующие учетные записи (4/4)	T1070 Устранение индикаторов (9/9)	T1111 Перехват мультимедиа (1/1)
T1594 Поиск на сайтах атакуемой организации (1/1)	T1588 Подготовка необходимых средств (2/8)	T1199 Доверительные отношения (1/1)	T1203 Эксплуатация уязвимостей в клиентском ПО (1/1)	T1136 Создание учетной записи (3/3)	T1134 Манипуляции с токенами доступа (5/5)	T1078 Существующие учетные записи (4/4)	T1187 Принудительная аутентификация (1/1)
T1595 Активное сканирование (3/3)	T1608 Размещение средств (1/1)	T1200 Подключение дополнительных устройств (1/1)	T1204 Выполнение с участием пользователя (2/3)	T1137 Запуск приложения Office (5/5)	T1484 Изменение доменной политики (2/2)	T1102 Изменение реестра (1/1)	T1212 Эксплуатация уязвимостей при получении учетных данных (1/1)
T1596 Поиск технической информации в общедоступных источниках (1/1)	T1550 Приобретение доступа (1/1)	T1566 Фишинг (2/3)	T1559 Микропроцессное взаимодействие (2/3)	T1170 Расширение браузеров (1/1)	T1543 Создание или изменение системных процессов (2/4)	T1127 Выполнение через доверенные утилиты разработчика (1/1)	T1528 Кража токена доступа (1/1)
T1597 Поиск в закрытых источниках (1/1)			T1569 Системные службы (1/2)	T1197 Задания BITS (1/1)	T1546 Выполнение по событию (4/16)	T1134 Манипуляции с токенами доступа (5/5)	T1539 Кража сессии (1/1)
T1598 Фишинг с целью сбора сведений (3/3)			T1609 Средства администрирования контейнера (1/1)	T1205 Передача управляющих сигналов в трафике (2/2)	T1547 Автозапуск при загрузке или входе в систему (12/14)	T1140 Деобфускирование/декодирование файлов или данных (1/1)	T1555 Утечка данных из паролей (3/5)
			T1610 Компонент серверного ПО (1/1)			T1197 Задания BITS (1/1)	T1556 Утечка данных из паролей (3/5)

рис.1 Матрица MITRE ATT&CK

Использование матрицы MITRE ATT&CK для анализа векторов атак помогает идентифицировать и оценить каждый потенциальный вектор на предмет его актуальности и опасности для организации. Это позволяет не только усилить оборону путем фокусировки на наиболее критических и вероятных направлениях атак, но и разработать более эффективные методы обнаружения и реагирования на инциденты. По мере того как поверхность атак расширяется и эволюционирует, интеграция знаний из матрицы MITRE в процесс управления киберрисками становится необходимым элементом защиты цифровых и физических активов организации.

## **2.2 Распространенные виды векторов атак**

### **2.2.1 Скомпрометированные учетные данные**

Злоумышленники используют скомпрометированные учетные данные для взлома приложений, систем, устройств и сетей. Они активно пытаются скомпрометировать учетные данные различными методами. Например, фишинговые атаки могут обманом заставить пользователей раскрыть свои учетные данные. Атака методом перебора подбирает разные комбинации логина и пароля, чтобы найти настоящие учетные данные.

### **2.2.2 Фишинг**

Фишинг — один из наиболее широко используемых векторов атак. Этот метод основан на социальном инжиниринге и направлен на то, чтобы обмануть пользователей, заставив их скачать вредоносные файлы, перейти по вредоносным ссылкам или раскрыть конфиденциальную информацию. Злоумышленники используют его для различных целей, таких как получение учетных данных, проведение атак с применением программ-вымогателей и кража финансовой информации.

### **2.2.3 Вредоносное ПО**

Вредоносное программное обеспечение (вредоносное ПО) служит вектором атаки, помогая злоумышленникам красть данные, взламывать системы и выполнять вредоносные задачи. Большинство вредоносных программ создается для достижения конкретных целей. Например, программы-вымогатели шифруют файлы и требуют выкуп в обмен на ключи шифрования, а шпионские программы отслеживают действия пользователей и отправляют эту информацию злоумышленникам.

### **2.2.4 Внутренние угрозы**

Внутренние угрозы действуют изнутри организации в качестве авторизованных пользователей. Это может быть сотрудник, который по

неосторожности раскрывает конфиденциальную информацию, например, учетные данные, актору социальной инженерии. Также существуют и вредоносные злоумышленники — сотрудники или бывшие сотрудники, которые намеренно злоупотребляют своими полномочиями для выполнения несанкционированных действий. Например, бывший сотрудник, чьи полномочия не были отозваны, может украсть коммерческую тайну и удалить эти файлы.

### 2.2.5 Эксплуатация уязвимостей

Уязвимость — это недостаток, который злоумышленники могут использовать для атаки на программное или аппаратное обеспечение. Существуют два основных типа уязвимостей: известные уязвимости, о которых сообщили публично, и уязвимости нулевого дня, которые являются неизвестными векторами. Злоумышленники используют оба типа для проведения атак, но уязвимости нулевого дня считаются более привлекательными, так как они дают злоумышленникам больше времени для атаки до того, как кто-либо узнает об их активности.

### 2.2.6 SQL-инъекция

SQL (язык структурированных запросов) — это язык программирования, позволяющий работать с базами данных. Многие серверы, хранящие конфиденциальные данные, используют SQL для управления данными. SQL-инъекция — это вектор атаки, который внедряет вредоносный SQL-запрос, чтобы заставить сервер выдать информацию.

Успешная SQL-инъекция, нацеленная на базы данных, содержащие номера кредитных карт, персонально идентифицирующую информацию (ПИ) или учетные данные, является нарушением требований кибербезопасности, которое представляет угрозу не только пользователям, но и бизнесу, которому принадлежит база данных, и поставщику ПО, который ею управляет.

## **2.3 Цифровые поверхности атак**

Цифровая поверхность атак включает все программное обеспечение, оборудование и сетевые компоненты, которые могут быть уязвимы для кибератак. Элементы цифровой поверхности атаки включают:

- Веб-приложения: веб-сайты и веб-сервисы, которые обрабатывают пользовательский ввод и взаимодействуют с базами данных.
- API (интерфейсы программирования приложений): API позволяют различным программным системам взаимодействовать, потенциально раскрывая конфиденциальную информацию, если они не защищены должным образом.
- Конечные точки: устройства, подключенные к сети, такие как ноутбуки, смартфоны, серверы и устройства IoT, которые могут быть использованы злоумышленниками для несанкционированного доступа или кражи данных.
- Сетевая инфраструктура: компоненты, такие как маршрутизаторы, коммутаторы и межсетевые экраны, которые управляют обменом данными между устройствами в сети; безопасные конфигурации необходимы, чтобы предотвратить распространение атак по всей сети.

## **2.4 Физические поверхности атак**

Физическая поверхность атак связана с рисками безопасности, касающимися материальных активов организации. Примеры включают:

- Дата-центры: физические помещения, в которых размещены серверы и другое оборудование; несанкционированный доступ может привести к краже или повреждению данных.

- Рабочие места сотрудников: настольные компьютеры, ноутбуки и мобильные устройства, используемые сотрудниками и являющиеся целями для кражи или взлома.
- Системы контроля доступа: меры безопасности, такие как электронные карты доступа, биометрические сканеры и камеры наблюдения, которые должны должным образом обслуживаться, чтобы предотвратить несанкционированный доступ в защищенные зоны.

## **2.5 Способы защиты от векторов атак**

- Внедрение надежной аутентификации:

Организации должны иметь политики паролей, чтобы обеспечить надежность и правильное хранение всех имен пользователей и паролей. Многофакторная аутентификация (MFA) должна быть обязательной, как минимум для чувствительных систем и административных аккаунтов, обеспечивая дополнительный уровень защиты.

- Проведение тестов на проникновение:

Тестирование на проникновение позволяет организациям выявлять, ранжировать и проверять уязвимости в системе безопасности. Обычно эти тесты проводит этичный хакер, либо как внутренний сотрудник, либо как внешний провайдер услуг. Тестировщики проникают в систему, используя методы злоумышленников, чтобы оценить взломоустойчивость сети, приложения или компьютера.

- Регулярные проверки и тестирование на уязвимости:

Организациям следует проводить тестирование на уязвимости ИТ-ресурсов не реже одного раза в квартал, привлекая внешних аудиторов к ежегодному тестированию. Проверки и тесты необходимы для выявления

уязвимостей ИТ-ресурсов и помогают обновлять контроли безопасности и политики.

- Обучение сотрудников:

Каждый новый сотрудник должен пройти комплексное обучение по ИТ-безопасности. Все сотрудники должны регулярно (не реже одного раза в год) проходить обучение, чтобы быть в курсе актуальных политик безопасности и передовых практик.

- Установка обновлений немедленно:

Отдел ИТ должен устанавливать обновления программного обеспечения, оборудования и прошивок сразу после их выхода. Устройства на местах должны автоматически получать обновления безопасности через механизм "push".

- Внедрение закрытой сети:

Существует несколько способов ограничить доступ к корпоративным системам и данным. Системы на основе облака удобны для удаленного доступа. Организации с политиками BYOD (использование собственных устройств) должны внедрить контроли для защиты своих систем, позволяя пользователям подключаться к сети через их устройства. Одна из стратегий — использовать виртуальные частные сети (VPN), чтобы ограничить доступ только определенному кругу пользователей без раскрытия данных в публичном Интернете.

- Шифрование данных на портативных устройствах:

Надежное шифрование данных важно для защиты информации на периферийных устройствах, таких как ноутбуки и смартфоны. Организации могут выбрать надежную технологию шифрования, такую как Advanced

Encryption Standard (AES), чтобы минимизировать риск компрометации данных.

- Применение физического контроля доступа:

Большинство взломов и утечек данных влияет на ИТ-инфраструктуру, но физическая инфраструктура также может быть вектором атаки. Злоумышленники могут проникнуть в физические пространства, где размещены чувствительные серверы, центры обработки данных и складские помещения. Организации должны защищать и контролировать доступ к своим физическим активам, включая филиалы, полевые сенсоры и картотеки.



## ГЛАВА 3

### СТРАТЕГИИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ: АНАЛИЗ И УПРАВЛЕНИЕ ПОВЕРХНОСТЬЮ АТАКИ

#### 3.1 Анализ и мониторинг поверхности атаки

Анализ поверхности атаки предполагает картирование всех векторов атаки в рамках организации. Это позволяет выявить зоны риска и уязвимые системы, чтобы минимизировать количество векторов атаки.

Анализ поверхности атаки помогает организациям определить области, нуждающиеся в более тщательном тестировании на уязвимости, и найти зоны повышенного риска для защиты вглубь. Также этот анализ можно использовать, чтобы понять, какие изменения в инфраструктуре создают новые изменения в поверхности атаки.

**Анализ поверхности атаки можно проводить двумя основными способами: вручную с помощью тестировщиков на проникновение и архитекторов безопасности, а также с помощью автоматизированных инструментов.** Программное обеспечение для управления поверхностью атаки может постоянно мониторить инфраструктуру на наличие новых и потенциальных уязвимостей и ошибок конфигурации.

#### 3.2 Минимизация цифровой поверхности атаки

Сетевая поверхность атаки включает все уязвимости и недостатки безопасности в подключенном программном и аппаратном обеспечении. Вот несколько способов помочь сократить цифровую поверхность атаки:

Сокращение объема исполняемого кода: чем больше кода выполняется в системе, тем выше вероятность, что в нем будет обнаружена уязвимость. Сокращение объема исполняемого кода поможет вам минимизировать поверхность атаки.

Микросегментация: эта техника позволяет разбить сеть на изолированные логические единицы, каждая из которых имеет собственную политику безопасности. Изоляция этих единиц помогает сдерживать угрозы в пределах одной единицы, предотвращая боковое перемещение злоумышленников.

### **3.3 Минимизация физической поверхности атаки**

Физическая поверхность атаки включает все конечные устройства в сети: настольные компьютеры, ноутбуки, USB-порты, мобильные устройства и жесткие диски. Злоумышленники, имеющие физический доступ к вычислительному устройству, могут использовать его для поиска точек входа в цифровую поверхность атаки, таких как стандартные настройки безопасности, не установленные обновления, неправильная конфигурация или уязвимости.

Физическую поверхность атаки могут использовать инсайдерские угрозы, такие как недобросовестные сотрудники, сотрудники, обманутые методами социальной инженерии, и злонамеренные злоумышленники, выдающие себя за работников сервиса. Она также подвержена внешним угрозам, например физическим взломам, небрежно утилизированному оборудованию с паролями и заметкам с паролями на стикерах.

### **3.4 Способ помочь сократить физическую поверхность атак**

**Контроль доступа и тестирование:** включает установку препятствий для предотвращения потенциальных взломов и усиление безопасности физических объектов от несчастных случаев, стихийных бедствий или атак. Например, можно использовать заборы, карты доступа, замки, системы пожаротушения и системы контроля доступа с биометрией.

**Наблюдение и уведомление:** предполагает установку камер наблюдения и систем оповещения для мониторинга физических объектов и предоставления предупреждений. Например, можно использовать датчики обнаружения вторжений, дымовые и тепловые детекторы.

**Восстановление после катастроф:** включает разработку политик и процедур восстановления после катастроф и регулярное их тестирование для обеспечения эффективности и актуальности. Эти политики могут помочь обеспечить безопасность и сократить время восстановления после разрушительных катастроф.

### **3.5 Снижение и управление поверхностью атаки**

Снижение и управление поверхностью атаки — это практика снижения поверхности атаки различными способами. Это предполагает постоянное оценивание поверхности атаки, исходя из понимания того, что она постоянно меняется и требует постоянной видимости. По мере лучшего понимания поверхности атаки вы можете предпринять шаги для ее уменьшения и защиты тех векторов, которые невозможно устранить.

### 3.5.1 Важность снижения поверхности атаки:

Раньше сети имели четкие границы, охраняемые межсетевыми экранами, и поверхность атаки существовала за этими границами. Однако современные сети сложные и хаотичные, не имеющие четких границ — угрозы существуют как внутри, так и снаружи. Поверхность атаки расширяется там, где находятся корпоративные данные, в состоянии покоя или при передаче.

Например, поверхность атаки организации может включать исходный код в репозиториях Azure, документы в Google Workspace, данные клиентов в SAP, хранилище и серверы на Amazon Web Services (AWS), электронные письма в Microsoft 365 и многое другое. Каждый из этих активов находится в разных частях экосистемы и может передавать данные между ними.

Такая поверхность атаки является реальностью современной корпоративной технологической архитектуры. Она обеспечивает гибкость и поддерживает удаленную работу, но создает все более сложную поверхность атаки. Проблему усугубляют новые парадигмы разработки ПО, такие как DevOps, и облачные технологии с микросервисами, значительно увеличивающие поверхность атаки.

### 3.5.2 Инструменты для снижения и управления поверхностью атаки:

Организации могут использовать различные инструменты для постоянного отслеживания поверхности атаки, определения существующих и меняющихся векторов атак, а также работы над их устранением или защитой

от них. Вот несколько инструментов, которые помогут обеспечить такой уровень видимости:

- **Управление инвентаризацией:** помогает организациям создать репозиторий известных систем. Обычно включает обнаружение активов для сканирования всех систем и ведения учета всех активов, включая теневое ИТ.
- **Управление уязвимостями:** эти инструменты сканируют внешние и внутренние системы на наличие известных уязвимостей. Это помогает расставить приоритеты, чтобы организации могли сначала устранить наиболее критические уязвимости.
- **Оценка внешних рисков:** включает в себя проведение сторонними организациями непрерывной оценки публичной безопасности организации.
- **Красные команды и тестирование на проникновение:** эти команды предоставляют экспертную информацию о векторах атак, которые позволяют злоумышленникам взломать цель. Эти данные помогают расставить приоритеты в наиболее актуальных векторах атак, чтобы снизить поверхность атаки.

### 3.5.3 Основные проблемы связаны с внешней поверхностью атаки

Основные проблемы, с которыми сталкиваются организации при попытке картирования и защиты внешней поверхности атаки:

- **Распределенные ИТ-экосистемы**

Организации больше не имеют традиционно четко определенного периметра сети. Современные ИТ-экосистемы включают многочисленные конечные точки и активы, разбросанные по разным местам и устройствам. Экосистема может включать основную сеть, региональные офисы, филиалы, сторонних хостинг-провайдеров и деловых партнеров, которые находятся за пределами корпоративных межсетевых экранов.

- **Теневые ИТ**

Помимо все более распределенного характера ИТ-экосистем, организации также сталкиваются с критическими рисками, связанными с теневыми ИТ — несанкционированным использованием ИТ-систем, программного обеспечения, устройств, услуг и приложений. Теневые ИТ часто помогают повысить производительность сотрудников и стимулируют инновации, но также вносят критические риски безопасности, что может привести к утечкам данных и потенциальным нарушениям нормативных требований.

Основная проблема не в том, что сотрудники используют какой-то конкретный инструмент, а в том, что проблемы с безопасностью возникают, когда сотрудники внедряют эти инструменты, не уведомив ИТ или отдел безопасности. Теневые ИТ означают, что команды безопасности даже не знают о скомпрометированных активах, которые уже эксплуатируются

злоумышленниками. Нет видимости, нет способа учесть все активы и гарантировать, что стек безопасности покрывает все компоненты, взаимодействующие с ИТ-экосистемой.

Если ИТ-отдел не знает об этих инструментах, он не может установить защиту вокруг них для обеспечения надлежащего использования и защиты от атак. Они не могут обновить программное обеспечение до последней безопасной версии или отслеживать уязвимости, из-за чего организация остается уязвимой для атак.

- **Чрезмерное количество данных из автоматизированных инструментов**

Организации часто используют несколько инструментов для мониторинга поверхности атаки. В результате они тратят значительные ресурсы и время, не добиваясь практически применимой видимости. Эти инструменты создают огромное количество данных, требующих постоянного анализа и обслуживания. Чрезмерное количество данных и слишком много оповещений могут в конечном итоге истощить ресурсы. Чтобы быть по-настоящему полезными, инструменты безопасности должны использовать механизмы приоритизации и отбора оповещений, чтобы предоставлять действенную аналитику.

## **ГЛАВА 4**

# **АРХИТЕКТУРА БЕЗОПАСНОСТИ: УПРАВЛЕНИЕ И ОПТИМИЗАЦИЯ ПОВЕРХНОСТИ АТАКИ**

### **4.1 Управление поверхностью атаки**

Даже небольшие организации могут иметь большую поверхность атаки. Чтобы все усложнить, эта поверхность постоянно меняется и растет. Переход на удаленную работу, растущая миграция рабочих нагрузок в облако и все более активное использование личных устройств для работы создают новые поверхности атаки, которые организации должны защищать.

Злоумышленники используют автоматизированные инструменты для разведки, чтобы проанализировать внешнюю поверхность атаки и найти уязвимые точки. Команды безопасности должны проводить тот же уровень оценки, чтобы понять свое воздействие на атаки. Таким образом, организациям необходимо использовать инструменты, обеспечивающие видимость и постоянный мониторинг, чтобы выявлять и устранять риски до того, как их обнаружат злоумышленники.

### **4.2 Инструменты управления поверхностью атаки**

Некоторые организации используют инструменты обнаружения активов для понимания своей расширенной ИТ-инфраструктуры. Однако, хотя эти инструменты полезны, они не могут полностью охватить поверхность атаки организации.

Инструменты обнаружения активов предоставляют только информацию об ИТ-активах внутри периметра безопасности компании. Большинство злоумышленников находится за пределами периметра, сканируя публичные системы организации на наличие уязвимостей. Решение для управления



поверхностью атаки заполняет этот пробел между тем, что видят внутренние системы, и тем, что могут использовать злоумышленники.

Инструменты управления поверхностью атаки могут помочь организации в:

- Определении видимых элементов инфраструктуры.
- Обнаружении теневого ИТ, артефактов от слияний и партнерских мероприятий, IoT-устройств и облачных преобразований.
- Выявлении киберсквоттинга, вредоносного ПО и активностей на теновом интернете.
- Поиске уязвимостей в обнаруженных активах.
- Оценке уязвимостей в соответствии с системой оценки рисков для определения приоритетов устранения.
- Помощи в реализации механизмов усиления безопасности, таких как сегментация сети, контроль доступа на основе ролей (RBAC) и модели безопасности Zero Trust.

#### **4.3 Метод и система сбора поверхностью атаки**

Метод и система сбора поверхности атаки для внешнего периметра организации являются процессом управления поверхностью атаки, направленным на анализ и улучшение кибербезопасности организации.

Ниже приведен процесс, по которому большинство инструментов управления поверхностью атаки обнаруживают активы, тестируют их на уязвимости, расставляют приоритеты рисков и устраняют их.

## **I. Обнаружение активов**

Невозможно управлять активом, не зная, что он существует. В современной цифровой среде существует много элементов, таких как устаревшие IP и учетные данные, теневое ИТ, облачные среды и IoT-устройства. Устаревшие инструменты и процессы легко пропускают такие активы, которые представляют собой важные поверхности атаки. Однако современные решения управления поверхностью атаки, использующие те же передовые методы разведки, что и злоумышленники, быстро обнаруживают их.

## **II. Добавление контекста**

Контекст и принадлежность активов — важная часть управления поверхностью атаки. Существующие инструменты обнаружения активов часто не предоставляют контекст в едином формате, что затрудняет приоритизацию устранения.

Эффективные методы управления поверхностью атаки дополняют информацию об активах, такую как IP-адрес, тип устройства, текущее использование, назначение, владелец, связь с другими активами и возможные уязвимости. Это позволяет командам безопасности расставлять приоритеты киберрисков и определять, следует ли удалять, обновлять, устранять или отслеживать активы.

## **III. Приоритизация**

Проверить и устранить весь список возможных векторов атаки на все активы практически невозможно. Поэтому важно уметь использовать контекстную информацию для определения фокуса и приоритетов. Команды

безопасности могут добавить критерии, такие как эксплуатируемость, возможность обнаружения, приоритеты злоумышленников и устранение, чтобы уделить внимание наиболее актуальным задачам.

#### **IV. Постоянное тестирование**

Проведение однократного тестирования поверхности атаки имеет ограниченную ценность, так как поверхность атаки растет и меняется каждый раз, когда добавляется новое устройство, учетная запись пользователя, рабочая нагрузка или сервис. Каждая новая учетная запись или устройство создает риск неправильной настройки, известных уязвимостей, уязвимостей нулевого дня и утечки конфиденциальных данных.

Важно непрерывно тестировать все возможные векторы атаки на всех поверхностях и всегда ссылаться на наиболее актуальную версию поверхности атаки организации.

#### **V. Устранение**

Как только поверхность атаки полностью картирована и контекстуализирована, можно начать устранять уязвимости. На основе приоритетов организация может устранять недостатки безопасности следующими способами:

- Автоматизированные инструменты: могут устранять некоторые типы уязвимостей без участия человека.
- Команды по обеспечению безопасности: ответственны за контроль рисков.
- ИТ-отделы: ответственны за работу затронутых систем.

- Разработчики: занимаются разработкой, обновлением и поддержанием активов и приложений.

Этим командам необходим контекст бизнес-рисков и четкие инструкции по устранению проблем безопасности, чтобы обеспечить доверие и эффективное решение задач.

#### **4.4 Программа управления поверхностью атаки**

Эффективная стратегия управления поверхностью атаки объединяет различные технологии и функциональные возможности безопасности для повышения эффективности и точности решений. При внедрении программы управления поверхностью атаки следует учитывать следующие элементы.

##### **I. Определение и приоритизация активов**

Первая часть программы управления поверхностью атаки — выявление активов, доступных из Интернета. Наличие четкой записи активов важно для классификации каждого актива на основе уровня риска, который он представляет для бизнеса. Один из способов классификации активов — установка заявлений о допустимых рисках и сравнение их с уровнем риска каждого актива. Следующим шагом будет определение приоритетов активов и внедрение соответствующих механизмов управления и политик устранения на основе рисков каждого актива.

##### **II. Рейтинги безопасности**

Рейтинги безопасности позволяют организациям постоянно отслеживать состояние своих ИТ-сред. Понимание состояния экосистемы имеет решающее значение для успеха программы управления поверхностью

атаки. Полная видимость цепочки поставок и сети позволяет компаниям быстрее выявлять уязвимости и минимизировать ИТ-поверхность атаки.

Рейтинги безопасности также полезны для постоянного мониторинга сторонних сред. Управление рисками сторонних организаций имеет решающее значение при работе с внешним поставщиком, поскольку уязвимости его безопасности влияют на его клиентов. Рейтинги безопасности помогают выявлять риски, связанные с партнерами и поставщиками, позволяя активно управлять поверхностью атаки каждого из них.

### **III. Сегментация сети**

Сегментация сети позволяет администраторам легче контролировать сетевой трафик и защищать активы. Разделение сети на отдельные управляемые части также облегчает обнаружение угроз. Это обеспечивает дополнительный уровень безопасности сети, гарантируя, что злоумышленники не смогут перемещаться по сети, даже если им удастся скомпрометировать один сегмент.

Сегментация сети часто включает контроль доступа, ограничивающий доступ к каждой части сети. Такой подход важен для внедрения безопасной среды Zero Trust.

### **IV. Сбор данных об угрозах**

Информация о киберугрозах предоставляет важные сведения об угрозах для организации, помогая разрабатывать меры защиты от потенциальных и текущих атак.

Данные о безопасности, собираемые средствами мониторинга, могут помочь выявить уязвимые места сети и приоритизировать высокорисковые угрозы. Ленты данных об угрозах отслеживают активность киберпреступников, что помогает обеспечить достаточный уровень безопасности вашей организации.

## ГЛАВА 5

### РИСК ОЦЕНКА ПОВЕРХНОСТИ АТАКИ ПОСЛЕ ВЫЯВЛЕНИЯ УЯЗВИМОСТИ

#### 5.1 Методология управления рисками

Управление рисками информационной безопасности предполагает применение разнообразных методик и моделей, каждая из которых направлена на минимизацию потенциального урона от реализации рисков.

Процессный подход к управлению рисками включает в себя четыре ключевых этапа: стратегическое планирование, активное внедрение, тщательный контроль и корректирующие действия. На стадии планирования происходит выбор стратегии управления рисками и оценка информационных активов, а также разработка профилей угроз. Этап внедрения предполагает реализацию систем безопасности в соответствии с планом и внесение изменений в бизнес-процессы с учетом рисков. Контроль заключается в проверке эффективности мер безопасности и функционирования контрольных механизмов. Завершающий этап — это анализ результатов мониторинга и аудита для усовершенствования управленческих процессов и обновления нормативной документации.

Модель **FRAP** фокусируется на качественном анализе рисков, акцентируя внимание на глубоком изучении информационной системы и выявлении угроз. Оценка рисков включает классификацию по вероятности возникновения и потенциальному ущербу.

Метод **CRAMM** является одним из наиболее авторитетных и широко применяемых подходов к оценке рисков, сочетающий в себе количественные

и качественные методы. Особое внимание уделяется оценке ценности информации и использованию шкалы баллов для оценки ущерба, а также классификации информационных ресурсов по типам угроз.

Модель **OCTAVE** также базируется на качественной оценке рисков и включает три фазы: подготовку, планирование и разработку стратегий. Основные аспекты модели — это создание индивидуального профиля угроз и точная идентификация уязвимостей для выбора наилучших стратегий информационной безопасности.

## **5.2 Методологии оценки рисков NIST**

**NIST (National Institute of Standards and Technology)** – это американский государственный институт, который разрабатывает стандарты и рекомендации для широкого спектра областей, включая кибербезопасность.

### **Риск-оценка уязвимостей по NIST:**

NIST предлагает фреймворк для оценки рисков, который включает в себя следующие этапы:

- Идентификация активов: Определите все ценные активы, которые необходимо защищать, такие как приложения, системы, данные, персонал, инфраструктура.
- Анализ угроз: Оцените потенциальные угрозы, которые могут нанести вред вашим активам.
- Оценка уязвимостей: Определите слабые места в ваших активах, которые могут быть использованы злоумышленниками.



- **Оценка вероятности и воздействия:** Оцените вероятность возникновения каждой угрозы и степень ее воздействия на ваши активы.
- **Определение рисков:** Умножьте вероятность возникновения каждой угрозы на ее воздействие, чтобы получить оценку риска.
- **Разработка мер по снижению риска:** Разработайте план действий по снижению рисков, например, путем устранения уязвимостей, внедрения мер контроля доступа, повышения осведомленности персонала и т.д.
- **Мониторинг и оценка:** Регулярно мониторьте ваши системы безопасности и переоценивайте риски, чтобы убедиться, что ваши меры по снижению риска остаются эффективными.

Вот несколько ключевых стандартов NIST, которые касаются оценки уязвимостей:

#### **NIST Cybersecurity Framework (CSF):**

**Функция идентификации:** Описывает процесс идентификации активов, а также выявления и анализа уязвимостей.

**Функция защиты:** Предоставляет рекомендации по выбору и реализации мер контроля для снижения рисков, связанных с уязвимостями.

#### **NIST Special Publication 800-53:**

**Раздел 4 “Безопасность и защита информации”:** Описывает меры контроля, которые должны быть реализованы для защиты конфиденциальности, целостности и доступности информации.

**Раздел 5 “Анализ рисков и управление рисками”:** Предоставляет руководство по оценке рисков, связанных с уязвимостями.

### **NIST Special Publication 800-30:**

Раздел 5 “Оценка рисков”: Предоставляет подробное описание процесса оценки рисков, включая методологии и инструменты для оценки вероятности и воздействия угроз.

### **NIST Special Publication 800-115:**

Раздел 3 “Оценка рисков”: Описывает методологии оценки рисков, которые можно использовать для оценки уязвимостей.

### **NIST Special Publication 800-160:**

Раздел 4 “Оценка и управление рисками”: Предоставляет руководство по управлению рисками, связанными с уязвимостями, включая оценку, минимизацию и мониторинг рисков.

Помимо этих стандартов, NIST также выпускает различные руководства, методические указания и ресурсы, которые могут помочь в оценке уязвимостей, например:

**NIST Cybersecurity Framework Implementation Tiers:** Описывает различные уровни зрелости кибербезопасности и предоставляет рекомендации по реализации CSF для различных организаций.

**NIST Risk Management Framework (RMF):** Предоставляет всеобъемлющий подход к управлению рисками, который включает в себя оценку уязвимостей.

Заключение:

Использование NIST для оценки уязвимостей – это хороший выбор для организаций, которые хотят убедиться в соответствии своих систем

безопасности международным стандартам. Однако необходимо учитывать сложность и ограничения NIST, а также использовать его в сочетании с другими методами оценки рисков.

### 5.3 Применение стандарта CVSS

#### **CVSS (Common Vulnerability Scoring System).**

CVSS представляет собой стандартизированную систему оценки уязвимостей, которая позволяет количественно оценить их важность и потенциальный ущерб для организации. Вот некоторые преимущества CVSS:

- Стандартизованность: CVSS предоставляет единый формат для оценки уязвимостей, что облегчает понимание и сравнение уровней риска между разными уязвимостями.
- Объективность: Методика CVSS основана на объективных критериях, что делает оценку уязвимостей менее субъективной и более надежной.
- Универсальность: CVSS подходит для оценки уязвимостей в различных типах систем и приложений, что делает его универсальным инструментом для оценки рисков.
- Гибкость: CVSS позволяет адаптировать оценку рисков в соответствии с конкретными потребностями организации, учитывая контекст использования уязвимости.

Чтобы провести оценку риска с использованием методики CVSS, вы можете использовать онлайн-калькуляторы CVSS или ручной подход, оценивая каждый измеряемый параметр уязвимости в соответствии с официальной документацией CVSS. После этого вы получите числовую оценку уязвимости, которая поможет вам приоритезировать действия по устранению уязвимостей и управлению рисками в вашей организации.

## 5.4 Практический анализ уязвимости на основе развернутого практического стенда и результата анализа поверхности

Если переходит от теории к практике. В рамках нашей работы была выявлена уязвимость CVE-2023-25690.

Давайте проанализируем уязвимость с идентификатором CVE-2023-25690 и оценим её риск на основе скоринговой системы NIST. ( 9.8 Score <https://nvd.nist.gov/vuln/detail/CVE-2023-25690>)

Идентификация уязвимости: CVE-2023-25690 описывает уязвимость в программном обеспечении, которое используется для обработки веб-запросов. Уязвимость позволяет удаленному злоумышленнику выполнить произвольный код на сервере, если он отправит специально сконструированный запрос.

### Оценка уязвимости:

*Вероятность эксплуатации:* Высокая. Уязвимость может быть эксплуатирована удалённо через интернет.

*Потенциальный ущерб:* Высокий. Успешное эксплуатация уязвимости может привести к выполнению произвольного кода на сервере, что может привести к утечке данных, нарушению целостности системы и даже полному контролю над сервером.

### Оценка риска:

На основе скоринговой системы NIST, данная уязвимость может быть оценена как высокий риск. Это объясняется как высокой вероятностью эксплуатации, так и значительным потенциальным ущербом.

Разработка стратегий смягчения рисков:

- Срочно применить патчи и обновления, предоставленные разработчиком программного обеспечения.

- Временно настроить дополнительные фильтры и правила брандмауэра для блокировки попыток эксплуатации уязвимости до применения патчей.
- Активировать мониторинг событий для выявления аномальной активности, связанной с попытками эксплуатации уязвимости.

#### Мониторинг и обновление:

Регулярно отслеживать обновления и новости от производителей программного обеспечения для быстрого реагирования на новые уязвимости.

После применения патчей периодически проводить сканирование системы на предмет обнаружения возможных уязвимостей или индикаторов компрометации.

### **5.5 Разработка стратегии управления рисками на основе риска аппетита компании и оценки риска ИТ инфраструктуры**

С одной стороны, эффективное управление рисками в области информационной безопасности требует адекватного понимания потенциальных угроз и уязвимостей в информационно-технологической (ИТ) инфраструктуре компании. С другой стороны, важно учитывать стратегические цели, бизнес-модель и риск аппетит компании, чтобы разработать подходящие стратегии управления рисками.

#### Сравнение риска аппетита компании и оценки риска ИТ инфраструктуры

Перед разработкой стратегии управления рисками необходимо провести сравнительный анализ риска аппетита компании и оценки риска ИТ

инфраструктуры. Для этого выясняются предпочтения и приоритеты компании в области безопасности информации, определяются потенциальные угрозы и уязвимости в ИТ инфраструктуре. Результаты оценки риска ИТ инфраструктуры, проведенной с использованием методов оценки уязвимостей, сопоставляются с уровнем терпимости к риску, установленным компанией.

### Разработка стратегии управления рисками

На основе сравнения риска аппетита компании и оценки риска ИТ инфраструктуры разрабатывается стратегия управления рисками. Эта стратегия должна учитывать уникальные потребности и цели компании, а также принимать во внимание область ее деятельности, степень вовлеченности в цифровые технологии и уровень риска, который компания готова принять или перенести. Определяются конкретные меры и политики безопасности, необходимые для уменьшения рисков в ИТ инфраструктуре и обеспечения соответствия рискам аппетита компании.

### Заключение

Разработка стратегии управления рисками на основе сравнения риска аппетита компании и оценки риска ИТ инфраструктуры представляет собой ключевой этап в обеспечении безопасности информации и успешного функционирования организации в цифровой среде. Правильно разработанная стратегия управления рисками позволяет компании эффективно адаптироваться к изменяющимся угрозам и уязвимостям, минимизировать риски и обеспечить сохранность ее активов и репутации.

## **ГЛАВА 6**

### **ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ МЕТОДА И СИСТЕМЫ СБОРА ПОВЕРХНОСТИ АТАКИ ДЛЯ ВНЕШНЕГО ПЕРИМЕТРА ОРГАНИЗАЦИИ**

#### **6.1. Вариант практической реализации применения метода и системы сбора поверхности атаки для внешнего периметра организации**

Поверхность атаки описывает все точки, через которые злоумышленник может проникнуть в систему или получить из нее данные.

Поверхность атаки включает:

- Все пути передачи данных/команд в и из приложения.
- Код, защищающий эти пути (авторизация, логирование, валидация данных и т.д.).
- Ценные данные, используемые в приложении (секреты, ключи, конфиденциальные данные).
- Код, защищающий эти данные (шифрование, контроль целостности и т.д.).

Эту модель следует накладывать на различные типы пользователей, которые могут получить доступ к системе (с разрешением или без). Чем больше типов пользователей, тем сложнее структура. Особое внимание следует уделять неавторизованным пользователям и привилегированным администраторам.

Группировка точек атаки:

- По уровню риска (внешние/внутренние).
- По назначению, технологии и дизайну.

Можно посчитать количество точек атаки каждого типа и выбрать некоторые из них для детального анализа.

Приложения на базе микросервисов и облачных технологий:

Такие приложения состоят из множества независимых компонентов, взаимодействующих через API. При оценке их поверхности атаки следует приоритизировать компоненты, доступные извне. Они могут быть скрыты за прокси, балансировщиками нагрузки или контроллерами входа, и масштабироваться без предупреждения.

## **6.2 Идентификация и картирование поверхности атаки**

Для демонстрации возможности сканирования поверхности, нами был реализован скрипт для автоматизации процесса идентификации и анализа потенциальных уязвимостей на внешнем периметре организации. Он выполняет сканирование сетевых ресурсов, извлекает контакты с веб-страниц и анализирует уязвимости с помощью различных инструментов.

Также для демонстрации функционирования программы был создан практический стенд, представляющий инфраструктуру организации, описанную ниже.



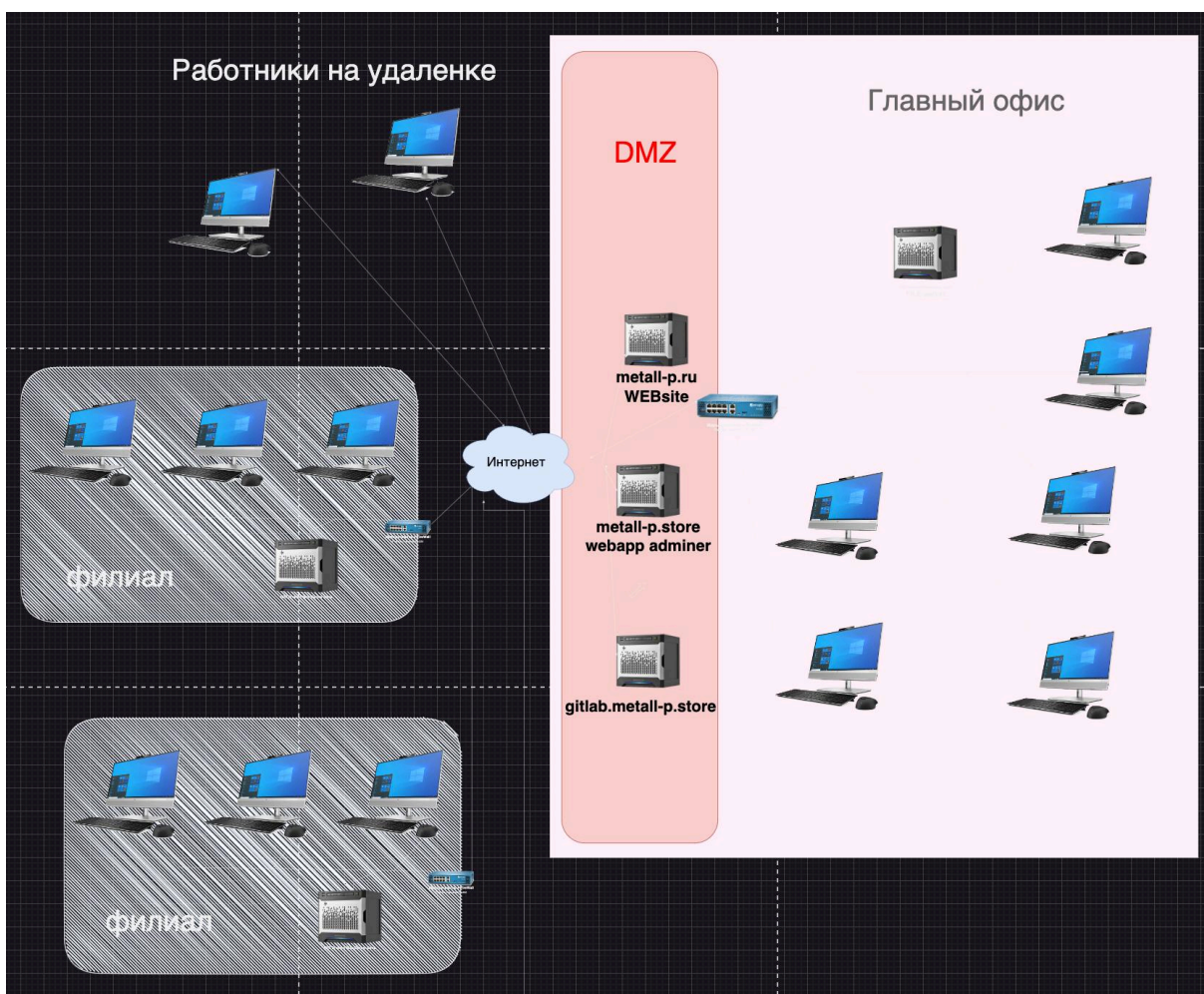


рис.2 Практический стенд (инфраструктура типовой организации)

Программа использует следующие инструменты и библиотеки:

- nmap: Инструмент сканирования сети, используемый для определения уязвимостей и сбора данных о целевых системах.
- gobuster: Инструмент для перебора директорий и поддоменов, что позволяет обнаруживать неизвестные/скрытые ресурсы на веб-сервере.
- requests и BeautifulSoup: Библиотеки Python для отправки HTTP-запросов и парсинга HTML-страниц соответственно. Используются для извлечения контактной информации с веб-страниц.

- re: Модуль регулярных выражений Python, предназначенный для фильтрации текста по специфическим шаблонам.

### 6.2.1 Описание работы программы:

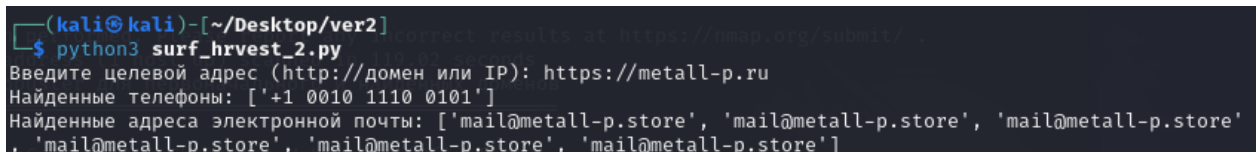
Программа начинает с запроса целевого адреса у пользователя. В зависимости от вида введенного адреса (IP или доменное имя), программа выбирает соответствующий метод анализа:

IP-адрес: Запускается сканирование с помощью nmap для определения открытых портов, сервисов и потенциальных уязвимостей на целевой системе.

Домен: Извлекается контактная информация с главной страницы домена, включая электронные адреса и телефоны. После чего выполняется сканирование nmap для доменов, полученных из адресов электронной почты, и сканирование gobuster для первоначального и всех найденных доменов для поиска дополнительных ресурсов.

### 6.2.2 Отчет по результатам сканирования поверхности атаки внешнего периметра организации:

- Инициализация сканирования



```
(kali@kali)-[~/Desktop/ver2]
$ python3 surf_hrvest_2.py
Введите целевой адрес (http://домен или IP): https://metall-p.ru
Найденные телефоны: ['+1 0010 1110 0101']
Найденные адреса электронной почты: ['mail@metall-p.store', 'mail@metall-p.store', 'mail@metall-p.store', 'mail@metall-p.store', 'mail@metall-p.store']
```

рис.3 Инициализация сканирования и сбор контактной информации

- Сбор контактной информации

Программа успешно извлекла следующие контактные данные с указанного веб-сайта, телефоны, адреса почт.

```
Запускаем скан nmap для домена: metall-p.store
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-18 08:39 EDT
Nmap scan report for metall-p.store (193.176.79.76)
Host is up (0.20s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux; protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:8.9p1:
|     CVE-2010-4816  5.0      https://vulners.com/cve/CVE-2010-4816
|     CVE-2023-51767 3.5      https://vulners.com/cve/CVE-2023-51767
80/tcp    open  http      WSGIServer/0.2 CPython/3.10.5
|_http-server-header: WSGIServer/0.2 CPython/3.10.5
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 500 Internal Server Error
|     Date: Sat, 18 May 2024 12:40:22 GMT
|     Server: WSGIServer/0.2 CPython/3.10.5
|     Content-Type: text/html
|     Content-Length: 135117
|     <!DOCTYPE html>
|     <html lang="en">
|     <head>
|       <meta http-equiv="content-type" content="text/html; charset=utf-8">
|       <meta name="robots" content="NONE,NOARCHIVE">
|       <title>IntegrityError
|     </title>
```

рис.4 Сканирование с помощью Nmap

- Сканирование с помощью Nmap

После определения доменного имени из адреса электронной почты , было запущено сканирование nmap для этого домена. Отчет nmap показал следующее:

```

8080/tcp open  http      Apache httpd 2.4.54 ((Debian))
|_http-server-header: Apache/2.4.54 (Debian)
| vulners:
|   cpe:/a:apache:http_server:2.4.54:
|   PACKETSTORM:176334      7.5      https://vulners.com/packetstorm/PACKETSTORM:176334      *EXPLOIT
*
|   OSV:BIT-APACHE-2023-25690      7.5      https://vulners.com/osv/OSV:BIT-APACHE-2023-25690
|   CVE-2023-25690      7.5      https://vulners.com/cve/CVE-2023-25690
|   5C1BB960-90C1-5EBF-9BEF-F58BFFDFEED9      7.5      https://vulners.com/githubexploit/5C1BB960-90C1-
5EBF-9BEF-F58BFFDFEED9      *EXPLOIT*
|   3F17CA20-788F-5C45-88B3-E12DB2979B7B      7.5      https://vulners.com/githubexploit/3F17CA20-788F-
5C45-88B3-E12DB2979B7B      *EXPLOIT*
|   1337DAY-ID-39214      7.5      https://vulners.com/zdt/1337DAY-ID-39214      *EXPLOIT*
|   OSV:BIT-2023-31122      6.4      https://vulners.com/osv/OSV:BIT-2023-31122
|   CVE-2017-12171      6.4      https://vulners.com/cve/CVE-2017-12171
|   OSV:BIT-APACHE-2022-36760      5.1      https://vulners.com/osv/OSV:BIT-APACHE-2022-36760
|   CVE-2022-36760      5.1      https://vulners.com/cve/CVE-2022-36760
|   OSV:BIT-APACHE-2023-45802      5.0      https://vulners.com/osv/OSV:BIT-APACHE-2023-45802
|   OSV:BIT-APACHE-2023-43622      5.0      https://vulners.com/osv/OSV:BIT-APACHE-2023-43622
|   OSV:BIT-APACHE-2023-31122      5.0      https://vulners.com/osv/OSV:BIT-APACHE-2023-31122
|   OSV:BIT-APACHE-2023-27522      5.0      https://vulners.com/osv/OSV:BIT-APACHE-2023-27522
|   OSV:BIT-APACHE-2022-37436      5.0      https://vulners.com/osv/OSV:BIT-APACHE-2022-37436
|   OSV:BIT-2023-45802      5.0      https://vulners.com/osv/OSV:BIT-2023-45802
|   OSV:BIT-2023-43622      5.0      https://vulners.com/osv/OSV:BIT-2023-43622
|   F7F6E599-CEF4-5E03-8E10-FE18C4101E38      5.0      https://vulners.com/githubexploit/F7F6E599-CEF4-
5E03-8E10-FE18C4101E38      *EXPLOIT*
|   E5C174E5-D6E8-56E0-8403-D287DE52EB3F      5.0      https://vulners.com/githubexploit/E5C174E5-D6E8-
56E0-8403-D287DE52EB3F      *EXPLOIT*
|   DB6E1BBD-08B1-574D-A351-7D6BB9898A4A      5.0      https://vulners.com/githubexploit/DB6E1BBD-08B1-
574D-A351-7D6BB9898A4A      *EXPLOIT*

```

рис.5 Пример результатов сканирования с выявлением множества критических уязвимостей

- Сканирование с помощью Gobuster

Было проведено сканирование gobuster для найденных доменов и поиск директорий.

```

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 120.32 seconds
Запускаем скан gobuster для первоначального и найденных доменов

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: https://metall-p.ru
[+] Method: GET
[+] Threads: 50
[+] Wordlist: big.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/.htaccess (Status: 403) [Size: 340]
/.bash_history (Status: 405) [Size: 167]
/.htpasswd (Status: 403) [Size: 340]
/admin (Status: 200) [Size: 273]

```

рис.6 Пример результатов сканирования с помощью Gobuster

```
/css      (Status: 301) [Size: 306] [→ http://metall-p.ru/css/]
/files    (Status: 301) [Size: 308] [→ http://metall-p.ru/files/]
```

рис.7 Пример результатов сканирования с помощью Gobuster

```
/images   (Status: 301) [Size: 309] [→ http://metall-p.ru/images/]
/js       (Status: 301) [Size: 305] [→ http://metall-p.ru/js/]
/robots.txt (Status: 200) [Size: 317]
```

рис.8 Пример результатов сканирования с помощью Gobuster

```
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Domain: metall-p.store
[+] Threads: 50
[+] Timeout: 1s
[+] Wordlist: big.txt

Starting gobuster in DNS enumeration mode

Progress: 20470 / 20471 (100.00%)

Finished
```

рис.9 Пример результатов сканирования с помощью Gobuster

**Видео работы программы на примере сбора поверхности атаки с практического стенд, представляющего инфраструктуру организации:**

<https://drive.google.com/file/d/12LjjhG2G6AvJwzpauoY48ox3nPj8JDwM/view?usp=sharing>

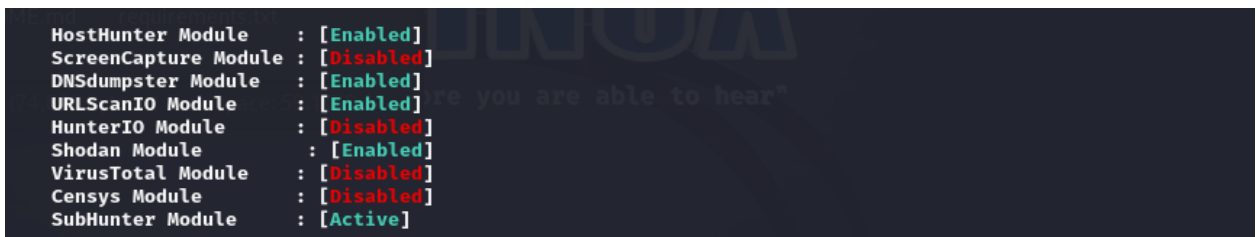
### 6.2.3 Дополнительные модули:

В данный скрипт можно добавлять дополнительные модули в зависимости от целей.

К примеру, пользователь может подать в систему домены, поддомены и IP-адреса, после чего скрипт применяет различные методы для выявления новых потенциальных целей. Это включает в себя перечисление поддоменов

с использованием методов грубой силы и пассивных запросов, анализ IP-адресов, принадлежащих одному сетевому блоку, а также IP, ассоциированных с множеством доменных имен.

После формирования полного списка целей, скрипт переходит к пассивной разведке: создает снимки веб-сайтов, составляет визуальные карты, ищет учетные данные в данных об общедоступных утечках, осуществляет пассивное сканирование портов с помощью сервисов **Shodan** и **Censys**, а также собирает информацию о сотрудниках через **LinkedIn**. Эта функциональность делает скрипт мощным инструментом в руках исследователей безопасности, стремящихся к максимальному расширению и анализу атакуемой поверхности.



```
HostHunter Module : [Enabled]
ScreenCapture Module : [Disabled]
DNSdumpster Module : [Enabled]
URLScanIO Module : [Enabled]
HunterIO Module : [Disabled]
Shodan Module : [Enabled]
VirusTotal Module : [Disabled]
Censys Module : [Disabled]
SubHunter Module : [Active]
```

рис.10 Вариант возможных модулей

### 6.3 Измерение и оценка поверхности атаки

После создания карты поверхности атаки необходимо определить зоны высокого риска. Далее принять меры по устранению уязвимостей и усилению защиты веб-ресурсов.

## **ЗАКЛЮЧЕНИЕ**

Анализ поверхности атаки является важной частью обеспечения безопасности приложения. Своевременное выявление рисков и непрерывный мониторинг изменений помогут разработчикам и специалистам по безопасности минимизировать воздействие кибератак и построить надежную защиту.

## **СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ**

1. Smith, John. "Managing Information Security Risks: A Practical Guide." Wiley, 2018.
2. Jones, Sarah. "Cybersecurity Frameworks: A Comprehensive Overview." Routledge, 2020.
3. Brown, David. "Introduction to Common Vulnerability Scoring System (CVSS)." O'Reilly, 2019.
4. National Institute of Standards and Technology. "NIST Cybersecurity Framework Version 1.1." NIST Special Publication 800-53, 2018.
5. Garcia, Maria. "Risk Management in Information Security: A Case Study Approach." Springer, 2017.
6. Johnson, Robert. "Principles of Risk Management and Insurance." Pearson, 2020.
7. National Cyber Security Centre. "Cyber Essentials: Introduction to Cyber Security." NCSC, 2019.



## Приложение 1. Код программы на языке Python

```
import subprocess

import re

import requests

from bs4 import BeautifulSoup

# Функция для запуска скана nmap

def run_nmap_scan(target):

    subprocess.run(['nmap', "-A", "--script", "vulners", "--script-args", "mincvss=3",
target], check=True)

# Функция для запуска скана gobuster

def run_gobuster_scan(target, wordlist):

    subprocess.run(['gobuster', 'dir', '-u', target, '-w', wordlist, '-t', '50'],
check=True)

# Функция для запуска скана gobuster для субдоменов

def run_gobuster_subdomains_scan(target, wordlist):

    result = subprocess.run(['gobuster', 'fuzz', '-u', f'FUZZ.{target}', '-w',
wordlist], capture_output=True, text=True)

    found_subdomains = [line.split()[-1] for line in result.stdout.splitlines() if
"Found:" in line]

    return found_subdomains

# Функция для извлечения адресов электронной почты и телефонов из веб-страницы

def extract_contacts(url):

    response = requests.get(url)

    soup = BeautifulSoup(response.text, 'html.parser')
```

```

    emails = re.findall(r'\b[A-Za-z0-9._%+-]+@[A-Za-z0-9.-]+\.[A-Z|a-z]{2,}\b',
str(soup))

    phones = re.findall(r'\+\d{1,3}\d{1,3}\d{1,3}', str(soup))

    return emails, phones

# Запрос целевого адреса

target = input("Введите целевой адрес (домен или IP): ")

# Проверка типа адреса и выполнение соответствующих действий
if re.match(r'\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}$', target):

    # Если адрес IP, запускаем скан nmap

    run_nmap_scan(target)
else:

    # Удаление http:// или https://, если они есть

    target = target.replace("http://", "").replace("https://", "")

    # Если домен, извлекаем контакты и почтовые адреса

    emails, phones = extract_contacts(f"http://{target}")

    print(f"Найденные телефоны: {phones}")

    print(f"Найденные адреса электронной почты: {emails}")

    # Из адресов почт выделяем домены и проверяем, отличаются ли они от вводного

    domains = set(email.split('@')[1] for email in emails)

    for domain in domains:

        if domain != target:

            print(f"Запускаем скан nmap для домена: {domain}")

            run_nmap_scan(domain)

    # Запускаем программу gobuster для первоначального и найденных доменов

```

```

print("Запускаем скан gobuster для первоначального и найденных доменов")

for domain in domains.union({target}):

    run_gobuster_scan(domain, '/Users/kostenko.evgeny/Desktop/1212/big.txt')

    subdomains = run_gobuster_subdomains_scan(domain,
'/Users/kostenko.evgeny/Desktop/1212/big.txt')

    if subdomains:

        print(f"Найденные субдомены для {domain}: {subdomains}")

# Сохранение результатов в txt файл
with open('scan_results.txt', 'w') as f:

    f.write(f"Результаты сканов для адреса: {target}\n")

    f.write(f"Найденные телефоны: {phones}\n")

    f.write(f"Найденные адреса электронной почты: {emails}\n")

    f.write("Результаты сканов nmap:\n")

    nmap_result = subprocess.run(['nmap', "-A", "--script", "vulners", "--script-args",
"mincvss=3", target], capture_output=True, text=True)

    f.write(nmap_result.stdout)

    f.write("Результаты сканов gobuster:\n")

    gobuster_result = subprocess.run(['gobuster', 'dir', '-u', target, '-w',
'/Users/kostenko.evgeny/Desktop/1212/big.txt', '-t', '50'], capture_output=True,
text=True)

    f.write(gobuster_result.stdout)

    f.write("Результаты сканов gobuster для субдоменов:\n")

    gobuster_subdomains_result = subprocess.run(['gobuster', 'fuzz', '-u',
f'FUZZ.{target}', '-w', '/Users/kostenko.evgeny/Desktop/1212/big.txt'],
capture_output=True, text=True)

    f.write(gobuster_subdomains_result.stdout)

```