**Адаптированная модель внешних угроз на основе   
MITRE ATT&CK для ООО "Гудфокаст"**

**Оглавление**

[**1.** **Модель внешних угроз** 3](#_Toc175224988)

[**1.1.** **Reconnaissance (Разведка)** 3](#_Toc175224989)

[**1.2.** **Resource Development (Подготовка ресурсов)** 3](#_Toc175224990)

[**1.3.** **Initial Access (Начальный доступ)** 4](#_Toc175224991)

[**1.4.** **Execution (Выполнение)** 4](#_Toc175224992)

[**1.5.** **Persistence (Закрепление)** 5](#_Toc175224993)

[**1.6.** **Privilege Escalation (Повышение привилегий)** 5](#_Toc175224994)

[**1.7.** **Defense Evasion (Уклонение от защиты)** 5](#_Toc175224995)

[**1.8.** **Credential Access (Доступ к учетным данным)** 5](#_Toc175224996)

[**1.9.** **Discovery (Разведка)** 6](#_Toc175224997)

[**1.10.** **Lateral Movement (Перемещение внутри сети)** 6](#_Toc175224998)

[**1.11.** **Collection (Сбор данных)** 6](#_Toc175224999)

[**1.12.** **Command and Control (Командование и контроль)** 6](#_Toc175225000)

[**1.13.** **Exfiltration (Эксплфильтрация данных)** 6](#_Toc175225001)

[**1.14.** **Impact (Воздействие)** 7](#_Toc175225002)

[**2.** **Дополнительные угрозы** 7](#_Toc175225003)

[**2.1.** **Сбор и продажа конфиденциальной информации** 7](#_Toc175225004)

[**2.2.** **Инсайдерские угрозы** 7](#_Toc175225005)

[**2.3.** **Подключение незарегистрированных устройств к корпоративной сети** 8](#_Toc175225006)

[**3.** **Приоритетные меры защиты** 8](#_Toc175225007)

[**3.1.** **Vulnerability management и Hardening** 8](#_Toc175225008)

[**3.2.** **Сегментация сети** 8](#_Toc175225009)

[**3.3.** **Ограничение привилегий** 8](#_Toc175225010)

[**3.4.** **Внедрение SIEM и EDR** 8](#_Toc175225011)

[**3.5.** **Повышение осведомленности сотрудников** 8](#_Toc175225012)

[**3.6.** **Контроль доступа к Wi-Fi и внешним устройствам** 8](#_Toc175225013)

[**3.7.** **Усиление защиты учетных записей** 9](#_Toc175225014)

[**Приложение Схема внешний поверхности атаки** 10](#_Toc175225015)

# **Модель внешних угроз**

## **Reconnaissance (Разведка)**

Phishing for Information (T1598). Фишинг с целью сбора сведений. Целевой фишинг через сторонние сервисы, фишинг с вложением, фишинг со ссылкой. Отправка писем сотрудникам со ссылкой на фишинговую страницу для компрометации учетных данных.

Search Open Websites/Domains: Code Repositories (T1593). Поиск на общедоступных сайтах: социальные сети, поисковые системы, репозитории кода.

***Рекомендации:***

*Регулярно обучать и тренировать сотрудников безопасно работать с внешними сервисами закрывать публичные доски, не оставлять персональные данные коллег в задачах и комментариях.*

*Регулярно обучать и тренировать разработчиков и девопсов правильно работать с секретами: создавать, ротировать, инвалидировать.*

*Если используется on-prem система контроля версий и она должна быть доступна удаленно, необходимо обеспечить к ней доступ только через защищенные каналы VPN с двухфакторной аутентификацией. Система должна быть настроена таким образом, чтобы все репозитории были приватными по умолчанию*

*Тренировать навыки сотрудников с помощью имитированных фишинговых атак.*

## **Resource Development (Подготовка ресурсов)**

Acquire Infrastructure (T1583). Злоумышленник обнаружил хостинг промо сайта, оплатил его и опубликовал на этом хостинге фишинговую страницу, которая имитирует вход в корпоративный портал.

***Рекомендации:***

*Описать и внедрить процесс управления активами, в том числе созданными доменами, промо сайтами и хостингом.*

*Использовать средства (EASM, ASM) для мониторинга внешней поверхности атаки.*

*Вовремя продлять или разделегировать все созданные домены, промо сайты и хостинг.*

*Наладить коммуникацию и слаженную работу между ITспециалистами, отделами маркетинга и безопасности.*

## **Initial Access (Начальный доступ)**

Phishing (T1566). Атаки с использованием фишинговых писем. Учитывая низкий уровень осведомленности персонала, фишинг представляет собой значительную угрозу, особенно для удаленных сотрудников.

Brute Force (T1110). Атаки методом перебора на сервисы, которые доступны извне (например, VPN серверы). Важно обратить внимание на этот аспект, так как есть угроза перебора учетных данных.

Exploitation of Public-Facing Applications (T1190). Потенциальная угроза для веб-сервисов и приложений, особенно если они будут связаны с внутренней инфраструктурой в будущем.

External Remote Services (T1133). Использование злоумышленниками уязвимостей в VPN для получения доступа к внутренней сети через удаленные рабочие станции.

Valid Accounts (T1078). Использование рабочий почты и пароля сотрудника для входа в корпоративные системы и получения доступа к данным клиентов компании.

***Рекомендации:***

*Регулярно обучать и тренировать сотрудников безопасно работать с внешними сервисами выбирать уникальные логины, придумывать сложные и разные пароли. А разработчиков не хранить пароли в открытом виде и писать безопасный код. В том числе, уметь использовать подготовленные выражения, безопасно и эффективно использовать ORM.*

*Описать и внедрить процесс управления тестовыми данными в ходе разработки: конфиденциальные и персональные данные клиентов не должны использоваться на тестовых стендах. Не публиковать тестовые среды на периметре, а держать их внутри за VPN.*

*Обучить команды инфраструктуры, разработки и тестирования безопасно готовить наборы тестовых данных для таких публикаций.*

*Описать и внедрить процесс управления паролями, который будет выполняться даже на тестовых средах*

## **Execution (Выполнение)**

Command and Scripting Interpreter (T1059). Использование злоумышленниками скриптов на удаленных рабочих станциях разработчиков и сотрудников, имеющих права локальных администраторов.

User Execution (T1204). Выполнение с участием пользователя. Запуск вредоносного ПО сотрудниками, особенно если есть доступ к интернету без контроля.

## **Persistence (Закрепление)**

Valid Accounts (T1078). Использование злоумышленниками украденных учетных данных сотрудников, имеющих локальные административные права, для закрепления в сети.

Boot or Logon Autostart Execution (T1547). Конфигурация автоматического выполнения вредоносного кода на системах с низким уровнем контроля доступа.

## **Privilege Escalation (Повышение привилегий)**

Valid Accounts (T1078). Использование рабочий почты и пароля сотрудника для входа в корпоративные системы и получения доступа к данным клиентов компании.

## **Defense Evasion (Уклонение от защиты)**

Obfuscated Files or Information (T1027). Использование маскировки кода для обхода антивирусного ПО, что может быть особенно критично до внедрения EDR.

Disable or Modify Tools (T1562). Отключение или модификация средств защиты, таких как антивирусное ПО, на рабочих станциях с правами администратора.

Valid Accounts (T1078). Использование логина и пароля сотрудника с повышенными привилегиями для входа в корпоративные системы и получения доступа к данным клиентов компании.

Hide Artifacts (T1564). Злоумышленники могут попытаться скрыть артефакты, связанные с их поведением, чтобы избежать обнаружения и также могут попытаться скрыть артефакты, связанные с вредоносным поведением, создавая вычислительные области, которые изолированы от общего инструментария безопасности.

## **Credential Access (Доступ к учетным данным)**

Brute Force (T1110). Применение атак brute force для получения доступа к учетным записям.

Credential Dumping (T1003). Извлечение учетных данных из памяти (например, с помощью инструментов типа Mimikatz, Impacket) на уязвимых системах.

Unsecured Credentials (T1552). Незащищенные учетные данные. Это могут быть учетные данные в файлах, учетные данные в реестре, история команд bash, закрытые ключи, API метаданных облачных экземпляров, параметры групповой политики, API контейнера, сообщения в переписках.

***Рекомендации:***

*Регулярно обучать и тренировать разработчиков и девопсов правильно работать с секретами: создавать, ротировать, инвалидировать.*

## **Discovery (Разведка)**

Network Service Scanning (T1046). Сканирование сети на предмет активных сервисов, что может быть выполнено после компрометации внешнего пользователя.

System Information Discovery (T1082). Сбор информации о системах, таких как установленные приложения и активные процессы.

## **Lateral Movement (Перемещение внутри сети)**

Remote Services (T1021). Использование удаленных сервисов (например, RDP) для перемещения внутри сети, особенно учитывая отсутствие сегментации.

Internal Spearphishing (T1534). Возможные фишинговые атаки внутри организации для перемещения к более защищенным системам.

## **Collection (Сбор данных)**

Data from Local System (T1005). Сбор данных с локальных систем, включая данные клиентов и конфиденциальную информацию.

Data from Information Repositories (T1213). Извлечение данных из баз данных и других хранилищ, особенно на серверах, содержащих конфиденциальную информацию.

## **Command and Control (Командование и контроль)**

C2 over Web Service (T1102). Использование веб-сервисов для связи с командным сервером, что может остаться незамеченным в условиях отсутствия SIEM.

Application Layer Protocol (T1071). Использование стандартных протоколов (например, HTTP/HTTPS) для связи с командным сервером.

## **Exfiltration (Эксплфильтрация данных)**

Exfiltration Over C2 Channel (T1041). Вывод данных через канал командования и контроля.

Exfiltration Over Web Service (T1567). Использование облачных сервисов для вывода данных.

## **Impact (Воздействие)**

Data Destruction (T1485). Возможность уничтожения данных на целевых системах, особенно если произойдет компрометация систем с критически важными данными.

Data Encryption for Impact (T1486). Шифрование данных с целью их удержания, например, при атаке с использованием шифровальщиков, как это уже происходило ранее.

Data Manipulation (T1565). Злоумышленник нашел уязвимость и украл все данные пользователей, включая логины и пароли в открытом виде.

Service Stop (T1489). Остановка службы. Есть риск полной остановки сервиса и бизнес процессов.

***Рекомендации:***

*Описать и внедрить процесс управления уязвимостями, процесс управления доступами, в том числе к внешним сервисам с возможностью самостоятельной регистрации, процесс работы с информацией, который определит, какие документы могут быть доступны всем внешним пользователям, а какие только сотрудникам компании и по отдельному согласованию. Проверить, что IT-команда понимает требования и внедрила эти процессы на всех корпоративных сервисах.*

*Организовать сегментацию сетей, проводить регулярный аудит систем и инвентаризацию пользователей.*

*Привлекать AppSec специалиста на этапе проектирования, чтобы не допускать появления уязвимостей.*

# **Дополнительные угрозы**

## **Сбор и продажа конфиденциальной информации**

В случае компрометации учетных данных или систем, злоумышленники могут пытаться извлечь и продать конфиденциальные данные клиентов или персональные данные. Это может привести к финансовым или репетиционным потерям.

## **Инсайдерские угрозы**

Возможность утечки информации или саботажа со стороны сотрудников, особенно учитывая отсутствие сегментации сети и контроля внешних устройств.

## **Подключение незарегистрированных устройств к корпоративной сети**

Риск несанкционированного доступа и утечки данных через Wi-Fi или другие способы подключения.

# **Приоритетные меры защиты**

## **Vulnerability management и Hardening**

Vulnerability management (Управление уязвимостями) — это непрерывный, циклический процесс выявления и устранения уязвимостей в инфраструктуре организации.

Он состоит из следующих этапов:

* Инвентаризация активов.
* Выявление уязвимостей.
* Выработка рекомендаций.
* Устранение уязвимостей.
* Контроль устранения уязвимостей.

Hardening - процесс настройки системы для повышения её безопасности путем уменьшения уязвимостей. Процесс включает в себя ряд мероприятий, направленных на минимизацию потенциальных рисков и атак, которым может подвергнуться система.

## **Сегментация сети**

Введение сегментации сети и ограничение доступа по ролям для минимизации рисков lateral movement (перемещение внутри сети).

## **Ограничение привилегий**

Настройка минимально необходимых прав для пользователей и приложений. Использование принципа наименьших привилегий (Principle of Least Privilege, PoLP) для ограничения доступа к ресурсам.

## **Внедрение SIEM и EDR**

Ускорение закупки и развертывания систем мониторинга и защиты конечных точек для повышения уровня обнаружения и реагирования на инциденты.

## **Повышение осведомленности сотрудников**

Проведение регулярных тренингов по кибербезопасности, особенно в части фишинга и безопасности работы с удаленными системами.

## **Контроль доступа к Wi-Fi и внешним устройствам**

Введение строгого контроля за подключением внешних устройств и разделением корпоративной сети на безопасные зоны.

## **Усиление защиты учетных записей**

Завершение внедрения двухфакторной аутентификации и строгий контроль доступа к учетным записям с высокими привилегиями.

# **Приложение Схема внешний поверхности атаки**

