



МЕТОДЫ ЗАЩИТЫ ОТ КИБЕРАТАК

Богомолова Дарья Александровна

студентка

научный руководитель: **Аверченко Артем Павлович**

ст. преподаватель

Омский Государственный Технический Университет, г. Омск

Введение

По мере развития информационных технологий, развивается и киберпреступность. Мошенники находят новые способы обхода служб безопасности. Каждый год увеличивается количество атак на различные организации, но самое страшное, что из-за киберпреступников, многие компании могут потерять контроль над своей базой данных. Также преступники активно интересуются сайтами правительства и военных структур, взлом которых может нанести непоправимый вред. Но попасться в ловушку мошенников могут и обычные пользователи интернета, которые где-то не обновили вовремя софт или поставили слишком ненадёжный пароль.

Цель работы

Суть работы заключается в том, чтобы рассказать читателям как можно избежать кибератак, какие существуют защиты от данного вида преступления и как применять на практике информацию, которую они получают.

Виды кибератак

Кибератаки могут осуществляться различными способами через компьютерные сети и системы. Для того, чтобы лучше понимать действия мошенников, необходимо разобраться в видах атак и в их ключевых способностях.

1. **DDoS-атаки.** Атаки вида «отказ в обслуживании» осуществляются за счет использования скомпрометированных компьютерных систем, которые направляют большое количество запросов к сайту или сети, что приводит к затрудненной работе на этом веб-сайте.

2. **Фишинг.** В фишинге мошенники используют электронные письма, замаскированные под письма компаний с хорошей репутацией. В этих фейковых сообщениях злоумышленники любыми способами пытаются получить доступ к личным данным. Давайте рассмотрим поддельные сайты, с помощью которых мошенники могут получить личные данные.

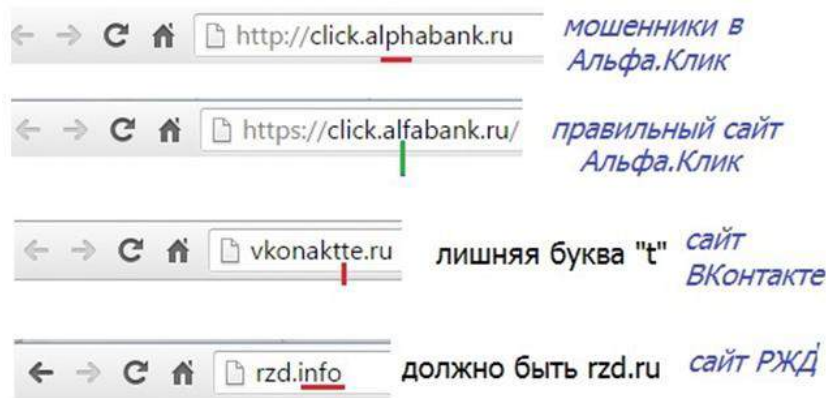


Рисунок 1

3. **Вредоносное ПО.** Данный термин охватывает любые виды программ, с помощью которых злоумышленник может получить доступ к вашим данным, либо причинить вред организации. К такому типу программ относятся трояны, компьютерные вирусы, черви.

4. **Атака посредника.** Атака посредника - это кража или искажение данных. При данном виде атаки злоумышленник тайно внедряется в коммуникацию двух людей с помощью незащищенного канала связи. В результате чего преступник может перехватить или подменить информацию.

5. **Взлом пароля.** Можно выделить три основных способа взлома пароля:

В первом случае хакер сам подбирает нужную комбинацию для входа в систему. Во втором случае используются специальные программы, которые генерируют миллиарды различных вариантов. В третьем случае хакер внедряет в компьютер вредоносное ПО, которое будет фиксировать нажатие клавиш при вводе пароля.

Итак, с видами кибератак мы ознакомились, но как защитить себя от данного вида преступлений?

Методы защиты от кибератак для организаций

1. Использование эффективных технических средств защиты:

- Системы централизованного управления обновлениями и патчами для используемого ПО;
- Систематизированная антивирусная защита с интегрированной средой для динамического мониторинга файлов;
- SIEM-решения;
- Использование автоматизированных средств анализа защищенности и выявления уязвимостей в ПО;
- Межсетевые экраны уровня приложений (webapplicationfirewalls);



- Системы глубокого анализа сетевого трафика;
- Специализированные сервисы анти-DDoS.

2. Защита данных:

- Избегайте хранения важной информации в открытом доступе;
- Регулярное создание резервных копий и их хранение отдельно от сетевых

элементов рабочей системы;

- Минимизирование привилегий пользователей и служб;
- Использование разных паролей для доступа к сайтам;
- Применение двухфакторной аутентификации во всех возможных зонах.

3. Избегание использование простых паролей:

- Применение парольной политики, которая рассматривает строгие требования к сложности и минимальной длине пароля;

- Регулярная смена пароля;
- Отказ от стандартных паролей.

4. Контроль безопасности систем:

- Своевременное обновление используемого ПО;
- Повышение осведомленности сотрудников в сфере информационной безопасности;

- Контроль появления небезопасных ресурсов на периметре сети;
- Регулярное проведение проверки защищенности веб-приложений;
- Отслеживание количества вопросов к ресурсам в секунду.

Методы защиты от кибератак для обычного пользователя

1. Использование ПО, которое имеет лицензию;
2. Использование эффективных средств антивирусной защиты;
3. Своевременное обновление ПО.
4. Хранение важной информации не только на жестком диске, но и в переносном носителе, облачном хранилище;
5. Применение учетных записей, которые лишены администраторских привилегий;
6. Использование двухфакторной аутентификации;
7. Использование сложных паролей, длиной не менее 8 символов;
8. Использование разных паролей для различных систем;
9. Регулярная смена паролей;
10. Внимательно просматривайте сайты, когда работаете с онлайн-платежами;
11. Не переходите по ссылкам из всплывающих окон;



12. Не загружайте файлы с подозрительных веб-ресурсов или из неизвестных источников.

Выводы

Ключевой задачей бизнеса является обеспечение информационной безопасностью. На сегодняшний день существует много способов борьбы с киберпреступностью, от компаний требуется лишь комплексный и проактивный подход к решению данной проблемы. Что касается обычных пользователей, соблюдение рекомендаций и осведомленность поможет избежать попадания в ловушки данных мошенников.

Список литературы:

1. [https://translated.turbopages.org/proxy_u/en-ru.ru.7d128907-63af167a-d48b6969-74722d776562/https/en.wikipedia.org/wiki/Attack_\(computing\)](https://translated.turbopages.org/proxy_u/en-ru.ru.7d128907-63af167a-d48b6969-74722d776562/https/en.wikipedia.org/wiki/Attack_(computing))
2. <https://onlanta.ru/press/smi/osnovnye-vidy-atak-na-infrastrukturu-i-kontseptsiya-zashchity-ot-nikh/>
3. <https://www.microsoft.com/ru-ru/security/business/security-101/what-is-a-cyberattack>