МЕТОДЫ ОБНАРУЖЕНИЯ И ОТКЛЮЧЕНИЯ НЕСАНКЦИОНИРОВАННО ПОДКЛЮЧЁННЫХ УСТРОЙСТВ К КОМПЬЮТЕРУ

Комалов Сергей Андреевич

студент, Национальный исследовательский университет «МИЭТ», РФ, г. Москва

Введение

В современном мире, где информационные технологии играют важную роль в повседневной жизни, безопасность компьютерного оборудования становится критически важным аспектом. Одной из проблем, с которой сталкиваются пользователи и администраторы, является использование несанкционированных устройств, подключенных к компьютеру. Такие устройства могут представлять угрозу для конфиденциальности данных и безопасности компьютера в целом. В данной статье рассматриваются методы обнаружения и нейтрализации таких устройств, их классификация, подходы к обнаружению и меры противодействия, а также практические рекомендации по усилению безопасности корпоративных сетей и персональных компьютеров.

Определение и классификация несанкционированных устройств

Несанкционированные устройства – это устройства, подключенные к компьютеру без разрешения администратора или владельца. Эти устройства могут использоваться для кражи данных, слежки или внедрения вредоносного кода.

Несанкционированные устройства можно классифицировать по различным критериям, таким как тип устройства, способ подключения и функциональное назначение.

Классификация по типу устройства:

- внешние накопители: флеш-накопители, жесткие диски и карты памяти;
- мобильные устройства: смартфоны, планшеты и электронные книги;
- устройства ввода-вывода: клавиатуры, мыши, сканеры и принтеры;
- сетевые устройства: Wi-Fi адаптеры, маршрутизаторы и модемы;
- аудио-видео устройства: микрофоны, камеры, наушники и колонки;
- внешние контроллеры: USB-хабы и контроллеры различных интерфейсов.

Классификация по способу подключения устройства:

- проводное: USB, HDMI, Ethernet, аудио разъемы и т.д.;
- беспроводное: Wi-Fi, Bluetooth, NFC, Zigbee и т.д.

Классификация по функциональному назначению:

- кража информации, сканирование системы и слежка;
- внедрение вредоносного кода;
- модификация данных, изменение настроек, удаление или изменение файлов;
- перехват трафика, анализ и модификация сетевого трафика и MITM-атаки.
- доступ к защищенным ресурсам, обход паролей или шифрования и доступ к закрытым данным.

Классификация несанкционированных устройств необходима для понимания их назначения,

Комалов С.А. МЕТОДЫ ОБНАРУЖЕНИЯ И ОТКЛЮЧЕНИЯ НЕСАНКЦИОНИРОВАННО ПОДКЛЮЧЁННЫХ УСТРОЙСТВ К КОМПЬЮТЕРУ // Студенческий форум: электрон. научн. журн. 2023. № 16(239). URL: https://nauchforum.ru/journal/stud/239/126095 (дата обращения: 05.09.2025).

возможных рисков и методов обнаружения. Чтобы предотвратить возможные угрозы безопасности, необходимо проводить регулярные проверки на предмет наличия несанкционированных подключённых устройств, а также использовать средства контроля и защиты.

Обнаружение несанкционированных устройств

Одним из самых простых способов обнаружения несанкционированных устройств является физический осмотр оборудования. Проверка портов и интерфейсов компьютера на наличие подключённых устройств может помочь обнаружить устройства, которые не должны быть подключены.

Хотя физический осмотр полезен для обнаружения несанкционированных устройств, его трудно выполнять регулярно, особенно в крупных организациях с большим количеством оборудования. Кроме того, физический осмотр требует значительного времени и ресурсов, а также специалистов, знакомых с широким типом устройств и потенциальными рисками их использования.

Для более эффективного обнаружения несанкционированных устройств существуют и другие методы, дополняющие физический осмотр или заменяющие его.

Существуют программные продукты, которые анализируют подключённые устройства, определяя их тип и характеристики. Они могут помочь выявить подозрительные устройства, которые представляют угрозу. Некоторые из этих программ предоставляют возможность сканирования всех подключенных устройств и формирования отчёта, который можно использовать для анализа и принятия решений о допустимости использования того или иного устройства.

Методы нейтрализации несанкционированных устройств

Если несанкционированное устройство обнаружено, его следует немедленно отключить. Важно также проверить систему на наличие вредоносного кода, который мог быть внедрен с помощью данного устройства. Рекомендуется провести антивирусное сканирование и, при необходимости, восстановить систему до состояния, предшествующего подключению устройства.

Для предотвращения подключения несанкционированных устройств можно блокировать доступ к физическим портам и интерфейсам. Это может выполняться с помощью специальных устройств-блокировщиков или программного обеспечения, которое контролирует доступ к портам. Блокировка портов может быть осуществлена на уровне BIOS или операционной системы с использованием специализированных инструментов и политик безопасности.

Ограничение прав доступа к компьютеру для определенных пользователей или групп пользователей поможет предотвратить подключение несанкционированных устройств. Это можно осуществить с помощью настроек операционной системы или средств управления доступом, таких как Active Directory или специализированных систем управления доступом.

Создание и внедрение системы мониторинга и контроля позволит снизить риск использования несанкционированных устройств и повысить общую безопасность. Система мониторинга и контроля должна включать следующие элементы:

- система обнаружения вторжений (IDS), которая может обнаружить подключение несанкционированных устройств и отобразить предупреждения;
- система программной блокировки несанкционированно подключённых устройств;
- система журналирования, которая может помочь провести анализ угроз.

Ниже представлены отечественные программные продукты, которые могут использоваться для создания и внедрения системы мониторинга и контроля подключения несанкционированных устройств:

DeviceLock – это российское решение для контроля доступа к съемным устройствам и портам на корпоративных компьютерах [1]. Оно позволяет администраторам устанавливать политики доступа на основе ролей и групп пользователей, а также мониторить и блокировать использование портов USB, FireWire, Bluetooth и других интерфейсов. DeviceLock интегрируется с системами аудита и журналирования для обеспечения полного контроля над подключаемыми устройствами.

Касперский Endpoint Security – решение для корпоративной среды, которое включает контроль доступа к съемным устройствам и блокировку портов. Касперский Endpoint Security помогает предотвратить утечку данных, обеспечивая гибкие настройки политик доступа и возможность аудита активности пользователей [2].

SoftActivity Monitor – это российское решение для мониторинга и контроля действий пользователей на корпоративных компьютерах [3]. Оно предоставляет администраторам возможность просматривать список подключённых USB-устройств, блокировать порты и удалять подозрительные устройства. Кроме того, SoftActivity Monitor позволяет мониторить активность пользователей в реальном времени, включая использование приложений, файлов и интернет-трафика.

LanAgent – это система контроля и учёта рабочего времени, которая обеспечивает защиту от утечек данных и подключения нежелательных устройств [4]. Она позволяет администраторам просматривать список подключённых устройств, блокировать порты и ограничивать доступ к определенным типам устройств.

StaffCop Enterprise – программное решение, предназначенное для мониторинга и контроля действий пользователей на корпоративных компьютерах, а также для обнаружения подключения несанкционированных устройств и предотвращения утечек данных [5].

InfoWatch ARMA Industrial EndPoint – программное решение от компании InfoWatch разработанное специально для промышленных предприятий и критически важных инфраструктур [6]. Это комплексное решение для защиты информации, обеспечивающее контроль над использованием съемных устройств, отслеживания действий пользователей и защиты от утечек данных.

Все вышеперечисленные российские программные продукты могут быть использованы для защиты корпоративных и частных компьютеров от потенциальных угроз, связанных с использованием несанкционированных устройств. Они позволяют администраторам эффективно контролировать подключение и использование различных устройств, предотвращая утечку данных и снижая риск нарушения безопасности.

Заключение

В современном мире, где безопасность компьютерных систем становится все более критически важной, использование несанкционированных устройств может представлять серьезную угрозу. Для обеспечения безопасности компьютеров необходимо использовать комплексный подход, включающий методы обнаружения и нейтрализации несанкционированных устройств, реализацию системы мониторинга и контроля, а также усиление политик безопасности. Это позволит защитить конфиденциальность данных, сохранить работоспособность систем и предотвратить утечки информации. Важно помнить, что обеспечение безопасности – это непрерывный процесс, который требует постоянного внимания и улучшения.

Список литературы:

1. Защита от утечек данных через мессенджеры и поддержка цифровых отпечатков в DeviceLock DLP [Электронный ресурс]. – Режим доступа: https://www.itweek.ru/security/article/detail.php?ID=200434 (дата обращения: 24.04.23)

2. Kaspersky Endpoint Security для бизнеса [Электронный ресурс]. – Режим доступа: https://www.kaspersky.ru/small-to-medium-business-security/endpoint-select (дата обращения: 24.04.23)

3. SoftActivity Monitor – Installation Guide for Administrators [Электронный ресурс]. – Режим доступа: https://www.softactivity.com/activity-monitor/docs/installation-guide/ (дата обращения: 24.04.23)

4. Как избежать утечки информации [Электронный ресурс]. – Режим доступа: https://lanagent.ru/kak-izbegat-utechki-informacii.html (дата обращения: 26.04.23)

5. Контроль USB-портов [Электронный ресурс]. – Режим доступа: https://www.staffcop.ru/enterprise/control-of-usb-devices (дата обращения: 26.04.23)

6. InfoWatch ARMA Industrial EndPoint – программное обеспечение, которое защищает АСУ ТП от угроз на уровне диспетчерского управления [Электронный ресурс]. – Режим доступа: https://www.infowatch.ru/products/zaschita-asu-tp-arma/zaschita-rabochikh-stantsiy-endpoint (дата обращения: 26.04.23)