|  |  |
| --- | --- |
|  | **Российский государственный социальный университет** |

**Рубежный контроль № 4.**

**по дисциплине «Информационная безопасность»**

**на тему «Вредоносное программное обеспечение (клавиатурные шпионы, AdWare программы, BHOпрограммы, Hijacker-программы, RootKit-технологии, Backdoor-программы, средства мониторинга, вымогательское ПО)»**

|  |  |
| --- | --- |
| **ФИО студента** | Салов Артём Владимирович |
| **Направление подготовки** | Программная инженерия |
| **Группа** | ПИН-Б-О-Д-2021-1 |

**Москва 2023**

Оглавление

[Введение. 3](#_Toc153745280)

[1. Вредоносное ПО. 4](#_Toc153745281)

[1.1. Что такое вредоносное ПО. 4](#_Toc153745282)

[1.2. Виды вредоносного ПО. 4](#_Toc153745283)

[1.3. Виды распространения. 5](#_Toc153745284)

[2. Противодействие вредоносному ПО. 6](#_Toc153745285)

[2.1. Профилактика вредоносного ПО. 6](#_Toc153745286)

[2.2. Избавление от вредоносного ПО. 7](#_Toc153745287)

[Заключение 8](#_Toc153745288)

# Введение.

Современное информационное общество, полагающееся на цифровые технологии, сталкивается с постоянной угрозой в виде вредоносного программного обеспечения (ВПО). Развитие информационных технологий и распространение цифровых устройств внесли свою долю удобства, но также подвергли нашу конфиденциальность и безопасность серьезным рискам.

Этот доклад посвящен разнообразным видам вредоносного программного обеспечения, охватывая такие угрозы, как клавиатурные шпионы, AdWare программы, BHO программы, Hijacker-программы, RootKit-технологии, Backdoor-программы, средства мониторинга и вымогательское ПО. Каждая из этих угроз представляет собой уникальный класс вредоносных программ, способных нанести серьезный ущерб как частным лицам, так и предприятиям.

В ходе этого исследования мы рассмотрим основные характеристики каждого вида вредоносного программного обеспечения, анализируя их распространение, функционал и возможные последствия. Цель этого доклада – предоставить полное представление о многообразии угроз и выработать рекомендации по обеспечению безопасности в цифровой среде, подвергающейся постоянным изменениям и усовершенствованиям киберпреступников.

# Вредоносное ПО.

## Что такое вредоносное ПО.

*Вредоносное программное обеспечение* (ВПО) представляет собой программы или код, созданные с прямой или скрытой целью причинения вреда компьютерным системам, данным или пользователям. Этот термин охватывает разнообразные виды вредоносных программ, каждая из которых предназначена для выполнения определенных функций, неблагоприятных для нормального функционирования системы.

## Виды вредоносного ПО.

* + 1. Клавиатурные шпионы:
* Описание: Клавиатурные шпионы, также известные как keyloggers, представляют собой программы, способные записывать нажатия клавиш на клавиатуре без ведома пользователя.
* Функционал:
  + Захват паролей, логинов и других конфиденциальных данных.
  + Мониторинг активности пользователя для кражи личной информации.
    1. AdWare программы:
* Описание: AdWare (рекламное программное обеспечение) представляет собой программы, цель которых показывать рекламу пользователям, часто внедряясь в браузер или приложения.
* Функционал:
  + Показ всплывающих окон и рекламных баннеров.
  + Сбор информации о предпочтениях пользователя для настройки рекламы.
    1. BHO программы (Browser Helper Object):
* Описание: BHO программы - это дополнительные модули, интегрированные в браузер, которые могут модифицировать его функционал.
* Функционал:
  + Изменение поведения браузера, например, перенаправление поисковых запросов.
  + Слежение за веб-активностью пользователя.
    1. Hijacker-программы:
* Описание: Hijacker-программы направляют пользователей на другие веб-сайты, отличные от тех, которые они собирались посетить.
* Функционал:
  + Изменение домашней страницы браузера.
  + Внедрение вредоносных расширений и панелей инструментов.
    1. RootKit-технологии:
* Описание: RootKit - это набор программ и технологий, предназначенных для скрытия присутствия вредоносного программного обеспечения в системе.
* Функционал:
  + Сокрытие процессов и файлов в системе.
  + Установка скрытых "задних дверей" для удаленного доступа.
    1. Backdoor-программы:
* Описание: Backdoor-программы создают скрытые точки входа в систему, обеспечивая злоумышленникам несанкционированный доступ.
* Функционал:
  + Удаленное управление компьютером без ведома пользователя.
  + Передача вредоносных файлов и программ на зараженное устройство.
    1. Средства мониторинга:
* Описание: Средства мониторинга используются для наблюдения за действиями пользователя без его согласия.
* Функционал:
  + Захват информации о посещенных веб-сайтах и использованных приложениях.
  + Регистрация чувствительных данных, таких как пароли.
    1. Вымогательское ПО (Ransomware):
* Описание: Вымогательское ПО блокирует доступ к данным или устройству, требуя выкуп для их разблокировки.
* Функционал:
  + Шифрование файлов на зараженном устройстве.
  + Отображение требований вымогателя с требованием выплаты для восстановления доступа.

Каждый вид ВПО представляет угрозу для конфиденциальности, целостности данных и функциональности системы, требуя эффективных мер по предотвращению и борьбе с этими угрозами.

## Виды распространения.

* + 1. Электронная почта (Email):
* Метод: Зловредные вложения или ссылки в электронных сообщениях.
* Описание: Злоумышленники могут отправлять электронные письма с вредоносными вложениями или ссылками, обманывая пользователей и заражая их устройства при открытии или переходе.
  + 1. Зараженные веб-сайты:
* Метод: Посещение веб-сайтов с вредоносным контентом.
* Описание: Вредоносные программы могут быть внедрены в веб-сайты, и пользователи могут заразиться при посещении этих сайтов или при взаимодействии с их содержимым.
  + 1. Зараженные носители данных (USB, внешние накопители):
* Метод: Передача ВПО через зараженные сменные носители данных.
* Описание: Вредоносные программы могут автоматически копироваться на устройства пользователя при подключении зараженного USB-накопителя, внешнего диска или других сменных носителей.
  + 1. Вредоносные веб-рекламы (Malvertising):
* Метод: Распространение через вредоносные рекламные баннеры на веб-сайтах.
* Описание: Атакующие могут размещать вредоносный код в рекламных баннерах, которые могут быть автоматически загружены при посещении определенных веб-сайтов.
  + 1. Эксплуатация программных уязвимостей (Exploits):
* Метод: Использование уязвимостей в программном обеспечении для внедрения ВПО.
* Описание: Злоумышленники ищут и эксплуатируют уязвимости в операционных системах, браузерах или других программах для внедрения ВПО без ведома пользователя.
  + 1. Социальная инженерия:
* Метод: Манипуляция пользователей для скачивания и установки ВПО.
* Описание: Злоумышленники могут использовать обман, фишинговые атаки или маскировку под надежные программы для убеждения пользователей в скачивании и установке ВПО.
  + 1. Пиратские копии программного обеспечения:
* Метод: Распространение ВПО через нелегальные версии программ.
* Описание: Злоумышленники иногда встраивают ВПО в пиратские копии программ, распространяемые через торренты или другие каналы.
  + 1. Файловые обменники и торренты:
* Метод: Распространение через сети файлового обмена.
* Описание: Вредоносные программы могут быть внедрены в файлы, предлагаемые для скачивания на пиратских или ненадежных файловых обменных площадках.

# Противодействие вредоносному ПО.

## Профилактика вредоносного ПО.

Профилактика вредоносного программного обеспечения (ВПО) является важным компонентом обеспечения безопасности информационных систем. Эффективные меры профилактики помогают предотвращать заражение устройств и снижают риск потери данных. Ниже приведены ключевые стратегии для профилактики ВПО:

* + 1. Использование Антивирусного программного обеспечения:
* Регулярно обновляйте антивирусное программное обеспечение на всех устройствах.
* Проводите систематические проверки на наличие вирусов и вредоносных программ.
  + 1. Обновление программного обеспечения:
* Убедитесь, что операционные системы, браузеры и другое программное обеспечение на устройствах всегда обновлены.
* Включите автоматические обновления, чтобы устранять уязвимости, которые могут использоваться злоумышленниками.
  + 1. Осторожность при Посещении Сайтов и Открытии Вложений:
* Избегайте посещения подозрительных веб-сайтов и кликайте только на проверенные ссылки.
* Не открывайте вложения в электронных письмах от незнакомых отправителей.
  + 1. Использование Брандмауэра:
* Активируйте брандмауэр на всех устройствах для мониторинга и фильтрации сетевого трафика.
* Конфигурируйте брандмауэр для блокировки нежелательного входящего и исходящего трафика.
  + 1. Обучение Персонала:
* Проводите регулярные обучающие программы для сотрудников о безопасности в сети, осведомленности о фишинге и техниках социальной инженерии.
  + 1. Регулярные Резервные Копии:
* Создавайте регулярные резервные копии данных, чтобы в случае заражения ВПО можно было быстро восстановить систему.
  + 1. Ограничение Прав Пользователей:
* Назначайте минимально необходимые права доступа пользователям, чтобы ограничить возможности ВПО в случае успешного проникновения.
  + 1. Использование Безопасных Паролей:
* Устанавливайте сильные пароли для всех учетных записей, чтобы затруднить попытки несанкционированного доступа.
  + 1. Мониторинг и Анализ Активности:
* Внедряйте системы мониторинга безопасности для раннего обнаружения подозрительной активности.
* Проводите регулярные аудиты безопасности.
  + 1. Создание Безопасного Сетевого Периметра:
* Разработайте и внедрите стратегии сетевой безопасности, включая использование виртуальных частных сетей (VPN) и других технологий для защиты данных при передаче по сети.

## Избавление от вредоносного ПО.

* + 1. Отключитесь от интернета

При отключении от интернета прекращается передача данных на сервер вредоносных программ, что позволяет защитить от заражения другие устройства. Если требуется подключиться к интернету для загрузки какого-либо инструмента, отключитесь сразу после его загрузки. Избегайте повторного подключения к интернету после получения требуемого инструмента. Перед отключением может оказаться полезным распечатать следующие инструкции.

* + 1. Перейдите в безопасный режим

Переход в безопасный режим позволит изолировать проблемы на устройстве.

* + 1. Не входите в учетные записи

Цель многих вредоносных программ – получение доступа к конфиденциальной информации обычно посредством кражи учетных данных, например, в результате отслеживания нажатий клавиш или считывания пароля с экрана или из буфера обмена. Избегайте входа в учетные записи, чтобы предотвратить потерю учетных данных.

* + 1. Удалите временные файлы

Вредоносные программы могут устанавливать на устройства временные файлы, которые необходимо удалить.

* + 1. Проверьте монитор активности

Если есть подозрение, что было установлено подозрительное обновление или приложение, закройте это приложение, если оно запущено. Монитор активности показывает запущенные на компьютере процессы и позволяет отслеживать их влияние на активность и производительность компьютера.

* + 1. Запустите поиск вредоносных программ

Средства поиска вредоносных программ позволяют удалить многие распространенные инфекции. Однако если на компьютере уже установлен и используется антивирус, рекомендуется использовать другое средство поиска вредоносных программ, поскольку текущее антивирусное решение может не обнаруживать эти вредоносные программы.

* + 1. Проверьте браузер

Вредоносные программы часто изменяют домашнюю страницу браузера, чтобы заразить компьютер повторно.

# Заключение

В современном цифровом мире, где технологии становятся неотъемлемой частью нашей повседневной жизни, вопросы безопасности и защиты данных приобретают все большее значение. Вредоносное программное обеспечение представляет серьезную угрозу для конфиденциальности, целостности и доступности информации, поэтому эффективные методы борьбы и профилактики имеют важное значение.

Проведенный анализ и изучение способов избавления от вредоносного программного обеспечения подчеркивают необходимость системного подхода к обеспечению безопасности. Регулярные апдейты программ, использование современных антивирусных и анти-малварных средств, а также обучение конечных пользователей основам кибербезопасности становятся ключевыми факторами в предотвращении и контроле угроз.

Важным аспектом также является понимание того, что безопасность - это процесс, а не одноразовое событие. Непрерывное мониторинг, анализ новых угроз и постоянное совершенствование стратегий защиты - залог успешной борьбы с вредоносным программным обеспечением.

С учетом постоянно меняющегося мира кибербезопасности, важно поддерживать внимание к текущим тенденциям и обновлять методы предотвращения и борьбы с угрозами. Только таким образом можно обеспечить стойкую защиту информационных систем и личной безопасности в цифровом мире.

*Список источников:*

1. Виды вредоносных программ – URL: <https://infobez.sakha.gov.ru/tpost/n0r2r08z01-vidi-vredonosnih-programm>
2. Вредоносное программное обеспечение – URL: <https://www.sberbank.ru/ru/person/kibrary/articles/vredonosnoe_programmnoe_obespechenie>
3. Вредоносное программное обеспечение: что это такое и как защититься от него – URL: <https://nauchniestati.ru/spravka/vredonosnoe-programmnoe-obespechenie/>
4. Методы защиты от вредоносных программ – URL: <https://studfile.net/preview/1636216/page:4/>
5. Как удалить вредоносные программы с компьютеров и Mac-устройств – URL: <https://www.kaspersky.ru/resource-center/threats/removing-malware>