**IT-Колледж “Сириус”**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**ДОКЛАД**

на тему “Антивирусы”

Выполнил:  
Студент группы

Группа 1.9.7.3  
Симонова Лора

Принял:

Старший преподаватель  
Тенигин Альберт Андреевич

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

IT-Колледж “Сириус”  
2022

Оглавление

[Введение 3](#_Toc122259179)

[Глава 1. 5](#_Toc122259180)

[Глава 2. 7](#_Toc122259181)

[Глава 3. 9](#_Toc122259182)

[Глава 4. 11](#_Toc122259183)

[Заключение 12](#_Toc122259184)

[Список используемых источников 13](#_Toc122259185)

# Введение

Антивирусы – приложения, защищающие от компьютерных вирусов, червей, троянов , бэкдоров, майнеров и т.д. Они бывают платные и бесплатные. Их метод работы заключается в том, что они следят за сетевым трафиком, прослушивают порты, контролируют службы, удаляют или “лечат” файлы и т.п.

Что такое вирусы, черви и трояны это понятно, но что такое майнеры и бэкдоры ?Про бэкдоры напишу чуть позже. Относительно недавно популярность набрали майнеры. Вирус-майнер – вредоносная программа обеспечения, основной целью которой является майнинг(т.е. заработок криптовалюты с использованием ресурсов вашего компьютера, условно это добыча нефти из скважены). Опасен он тем, что нарушает работу нашего пк, снижает производительность и скорее всего может вызвать перегрев , если работает он на 100%. Также майнер можно скачать уже готовый или Builder . (после того как вы скачали и почти все сделали вам надо указывать ссылку на сайт и понятное дело ввести свою карту). Как он вообще работает. Допустим есть сайт (в котором майнер) с которого вы что-то загрузили и он при попадании в систему получает доступ к ресурсам. Видеокарта и процессор нагреваются до предела, тот кто его создал просто получают прибыль в биткоинах. Т.е. заработок осуществляется на мощности ПК.

А как они так их находят?

Они находят вирусы, смотря код программы, реестр, список распространенных вирусов или даже могут просматривать Интернет, а все для того чтобы узнать, распределили ли его другие люди/программное обеспечение как вирус. Базы данных антивирусов содержат куски кодов **известных** вирусов.  Просто они сравнивают этот программный код по этой же базе и она на 100% позволяет определить есть вирус или нет. Конечно создаются и новые вирусы и при помощи этой базы уже их не определить. Поэтому антивирусники регулярно обновляются, т.к. вирусы не стоят на месте и всегда появляются новые.

# Глава 1.

Как вообще действуют антивирусы?

Приведу пример, файловый антивирус, находящийся в оперативной памяти, постоянно проверят все файлы, которые открываются, сохраняются или же запускаются.

Процесс проверки файла:

1.Антивирус получает информацию о файле сайта на базах iSwift (имеет ограничения , такие как :она не может проверять большие файлы ,у нее должно быть конкретное местоположение , расположенным в NTFS) и iChecker (увеличивает скорость проверки). После чего

2. Он анализирует на наличие вирусов как раз таки на базах. А вот базы содержат описание всех там на данный момент известных угроз, атак и т.д.

И выяснив это он поступает следующим образом:

1.Если он находит вредоносный код в файле сайта ,то он его блокирует , затем копию помещает в резервное хранилище и проводит так называемое “лечение”. После “лечения” он становится уже доступным и безопасным для работы. А если его не “вылечили” , то файл сата удаляется.

2. Если он обнаруживает этот код и не знает вредоносный он или нет , то отправляет этот файлик в специальное хранилище “карантин” , лечит его либо ,но если оказался безопасным, то он становится доступным для работы.

Что делает вредоносный код?

Он осуществляет бэкдор ( переводится как тайный вход и получает доступ к данным),состоит из двух частей

1. Вредоносный код
2. Открытый канал связи , при помощи которого атакующий может отправлять команду бэкдору (канал связи совокупность средств, позволяющий передавать сигналы к пользователю/получателю)

Примеры: eval

create\_function

preg\_replace

assert

base64\_decode и т.д. (хочу отметить такие примеры бэкдоров не требуют использования PHP).

# Глава 2.

На данный момент у многих есть встроенный антивирус на пк. Кроме того сейчас на приложениях Yandex, Chrome и т.д. тоже есть свой антивирусы. Но хочу сказать, что они не на все 100% защищают пк . Т.е. они слабые и могут не увидеть некоторые угрозы. Можно установить посторонние антивирусы их очень большое количество, главное не скачать какой-нибудь лжеантивирус. Главное тоже обновлять антивирусную базу данных, антивирусный сканер и т.д. чтоб избежать заражения.

К примеру приведу 3 антивируса:

*Касперский Internet Security*

* Создателями является Лаборатория Касперского.
* Язык программирования этого антивируса C++
* Он поддерживает все платформы, т.е. кроссплатформленный (IOS,MacOS,Android и т.д.) его можно установить как на пк , так и на телефоне.
* Создание в 2000 году .
* Последняя версия его 2021 года

Функции выполняет в принципе как и антивирус т.е.

Защищает от взлома устройства

платежи ( когда мы проводим онлайн-платеж на пк и телефоне он включает защиту и никто не сможет скопировать ваши данные карт и не узнают о платеже)

приложения ( к примеру на базе Android,получается приложение можно разблокировать только при помощи отпетчатка пальца,пароля или графического ключа)

домашней сети (если кто-то подключится можно будет видеть его данные , к примеру с какого устройства и т.д.)

облачное хранилище (тут думаю понятно обеспечивает безопасность облака ) и т.п.

Из минусов бы возможно отметила что скорость самого антивируса не очень высокая. И здесь возможно он будет защищать на 100% , но плюс в том , что его постоянно обновляют.

# Глава 3.

Второй антивирус 360 Total Security

* Платформы поддерживает Windows, Mac OS , Android.  
  (X86, X64)
* Имеет 5 антивирусных движков
* Создание 2008
* Последняя версия 2022
* Разработчик Qihoo

В нем находится основных 5 движка , отвечающие за отдельные компоненты . 2 лучших (Avira и Bitdefender)

1. Avira

Это мощный движок . У него высокая уровневая защита , что даже производит ложные срабатывания. Написан на java . Данная технология именуется AHeAD - Advanced Heuristic Analysis and Detection. Вообще он выключен по умолчанию, но его можно включить. За что он отвечает? Его функция защищать пароли , чтоб никто не смог копировать твои данные или взломать. Особенно не безопасно сохранение паролей в браузере.

1. Bitdefender

Этот движок тоже выключен по умолчанию. Он обеспечивает защиту почты. Он кидает полученные подозрительные письма в спам . Могут присылать разные сообщение в виде документа HTML, в который встроен троян к примеру. Естественно даже установленные антивирусы , которые рассчитаны на проверку файлов не всегда могут анализировать поток данных электронной почты. И если он не выполняет эту автоматическую проверку всех открываемых файлов , то вирус или троян все таки попадет на ПК.

1. 360 Cloud

Этот движок уже включен и его нельзя отключить. Он обеспечивает защиту

облачного хранилища.

4.QVM AI

Такая же история как и с 3 он всегда включен. По сути он защищает от неизвестных угроз и плюс в том ,что он предоставляет системе получить защиту от угрозы, с которой еще не знаком и у 360 total security является самостоятельным движком.

5.System repair . Это восстанавливающий движок предназначен для комплексной оценки и быстрого восстановления изменений операционной системы Windows.

# Глава 4.

Последний Avast.

* Язык программирования C++
* ОС: Windows, Android, IOS, Mac OS
* Cоздание в 1988 году

Хочу отметить , что есть Avast бесплатный и платный . Беслатная программа Avast очень уязвимая, в каком плане , возможно некоторым известно , что она при установке она копировала данные и продавала их компаниям (Google, Microsoft, McKinsey, TripAdvisor, Yelp, Conde Nast, The Home Depot, Pepsi и др.) Потому что он имеет право создавать резервную копию пользователя и может восстановить при обновлении пк либо же переустановке операционной системы.

В основном он выполняет такие же функции как и остальные антивирусы(червей, троянов и т.д.)

* Автоблокировка подозрительных сайтов
* Защита веб-камеры
* Облачная защита
* Интернет-защита
* Электронной почты и т.п.

# Заключение

Если вы определись, что вам нужно скачать антивирус , то даже здесь нужно быть бдительным и выбрать какой скачать , потому что есть такие как лжеантивирусы. Что они делают вприципе, такие программы яко бы выполняют функции обычного антивирусника, но на самом деле постоянно приходят оповещения с целью оплатить программу. Безусловно они копируют данные карты. Также не ограничивается это в краже паролей от важных онлайн-сервисов.

# Список используемых источников

1. Kaspersky Total Security. — Текст : электронный // Лаборатория Касперского : [сайт]. — URL: <https://www.kaspersky.ru/> (дата обращения: 18.12.2022).
2. Обзор антивируса 360 Total Security. — Текст : электронный // Хабр : [сайт]. — URL: <https://habr.com/ru/company/360totalsecurity/blog/280003/> (дата обращения: 21.12.2022).
3. Технологии. — Текст : электронный // Avast : [сайт]. — URL: <https://www.avast.ru/technology> (дата обращения: 21.12.2022).