Государственное бюджетное профессиональное образовательное учреждение

«Нижегородский радиотехнический колледж»

**ПОЯСНИТЕЛЬНАЯ ЗАПИСКА**

**ИНДИВИДУАЛЬНОГО ПРОЕКТА**

**«Создание Антивируса»**

**Авторы проекта:**

Пронин Д.А. (1ИСиП-22-2)

Сальникова А.Д.(1ИСиП-22-2)

**Кураторы:**

Калачёв А.А.

Пигалова Н.В

Нижний Новгород

2022

**Оглавление**

**Введение..................................................................................................................................2**

**Глава 1. Принципа работы антивирусных программ1.Что такое антивирус? 3**

**1.2 Методы защиты от вирусов 4**

**1.3 Классификации антивирусных программ 5**

**Глава 2. Создание антивируса. 2.1 Выполнение работы 7**

**2.2 Ход работы. 7**

**Заключение 9**

**Список литературы.............................................................................................................10**

**Приложение..........................................................................................................................11**

**ВВЕДЕНИЕ**

**Актуальность:** в настоящее время компьютер прочно вошел в нашу жизнь. Его возможности используются на работе, учебе, при проведении досуга, в быту и других сферах жизни человека. Количество информации, которую люди доверяют своему «электронному другу», с каждым днем увеличивается, поэтому рано или поздно каждый задается вопросом: «Как обеспечить надежную сохранность данных?» Несмотря на широкую распространенность антивирусных программ, вирусы продолжают «плодиться». Чтобы справиться с ними, нам необходимо создавать более универсальный и качественно-новый антивирус, который будет включать в себя все положительные качества своих предшественников. Компьютер играет в жизни человека огромную роль, поскольку он помогает ему во всех областях его деятельности. Современное общество все больше вовлекается в виртуальный мир Интернета. Но с активным развитием глобальных сетей актуальным является вопрос информационной безопасности, так как проникающие из сети вирусы могут нарушить целостность и сохранность информации в наших компьютерах. В последние время, люди стали пользоваться программами с непроверенных источников, тем самым отравляя свои гаджеты. И сейчас противоядием в компьютерном мире стали программы, называемые антивирусными. Поэтому на любом современном компьютере должна быть обязательно установлена антивирусная программа.

**Объект исследования** являются компьютерные вирусные угрозы и антивирусное программное обеспечение.

**Предмет исследования** являются методы борьбы с компьютерными вирусными угрозами путем использования аппаратно-программных способов.

**Проблема**. В современном мире, несмотря на большие результаты в исследовании компьютерных вирусов, до сих пор не существует общепринятого и единого определения для данного типа информационных воздействий. Антивирусы со временем становятся уязвимы к новым вирусам. И вся информация с вашего компьютера попадает в руки мошенников, а иногда компьютеры просто ломаются.

**Цель работы.** Провести исследование и создать антивирусную программу.

**Задачи проекта**.

1. раскрыть основные понятия антивирусных программ;

2. изучить разновидности и типы антивирусных программ;

3. раскрыть и проанализировать наиболее популярные антивирусные программы.

4. создать программу антивируса на Python.

5. создать сайт для антивируса.

**Методы.**

1. обобщение различных источников по теме, взятых из Интернета и дополнительной литературы;

2. сопоставление различных антивирусных программ;

3. анализ опроса в интернете.

**Продукт.** Антивирус.

**ГЛАВА 1. ПРИНЦИП РАБОТЫ АНТИВИРУСНЫХ ПРОГРАММ**

1.Что такое антивирус?

**Антивирус** — это специализированная программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ и восстановления файлов, зараженных (модифицированных) такими программами, а также предотвращения - предотвращения заражения (изменения) файлов или операционной системы вредоносным кодом. В своей работе эти программы используют различные политики для поиска и лечения зараженных файлов. Чтобы нормально работать на компьютере, каждый пользователь должен следить за обновлением антивируса.

Также стоит отметить наличие псевдовирусов. В 2009 году началось активное распространение программного обеспечения, которое не является антивирусным (то есть не имеет реальной функциональности для борьбы с вредоносным ПО), но выдает себя за него. На самом деле антивирусные программы на основе файлов могут быть как программами для обмана пользователей и получения прибыли в виде платы за "лечение системы от вирусов", так и обычными вредоносными программами.

1.2 Методы защиты от вирусов

Авторы вредоносных программ регулярно обновляют и улучшают свою среду, поэтому существует острая необходимость в создании антивирусов самостоятельно, поэтому появляется множество способов защиты от вируса.

Системная сигнатура (анализ сигнатур, метод подписи) содержит файлы для поиска специальной последовательности байтов — символа подписи для конкретного вируса. Для каждого вновь обнаруженного вируса специалисты антивирусной лаборатории анализируют код, на основе которого определяется его сигнатура. Выходной код помещается в специальный список вирусных сигнатур, где активен антивирус. Преимуществом этого метода является очень низкий процент ложных срабатываний, а самая главная невозможность - найти новый вирус в системе, где в базе данных антивируса нет сигнатуры, поэтому требуется трудоемкое обновление базы данных сигнатур.

Любое неожиданное изменение в методе управления целостностью требует особого внимания к данным на диске благодаря антивирусной системе и ее существованию в качестве подозрительной вирусной основы (изменение существующих данных (особенно обработанных или исполнительных файлов), видимость новых исполнительных файлов, разное). На самом деле преобразование данных — нарушение преобразования данных - упрощается путем сравнения исходного варианта кода в рамках теста с предварительно вычисленной контрольной суммой (дайджест) и текущего варианта кода в рамках теста с контрольной суммой (дайджест). Если они не подходят, нарушение нарушено и есть все основания провести дальнейшую аутентификацию этого кода, например, просканировать сигнатуру вируса. Этот метод работает быстрее, чем метод сканирования сигнатур, поскольку для вычисления контрольной суммы требуется малобайтовое сравнение фрагментов кода и позволяет находить следы любой функции, включая неизвестные вирусы, у которых нет сигнатуры в базе данных.

Способ сканирования подозрительных команд (высокое сканирование, эвристический режим) основан на идентификации подозрительных команд и (или) подозрительных символов кодовой последовательности (например, команды форматирования жесткого диска или встроенной функции в активной программе или исполняемом коде) в сканируемом файле. После этого делается вывод о вредоносной природе файла и предпринимаются дополнительные действия для его проверки. Этот метод обладает хорошей производительностью, но часто не позволяет обнаружить новые бактерии.

Способ отслеживания поведения программ основан на анализе поведения, запускаемого программами с помощью этого метода, основанного на методах сканирования содержимого файлов, упомянутых ранее, и сопоставимых "ручных" на месте преступления для поимки преступника. Эти типы антивирусных инструментов часто требуют активного участия пользователя, которого просят принять решение в ответ на многочисленные системные предупреждения, важная часть которых позже может превратиться в ложные срабатывания. Когда уровень ложных срабатываний превышает лимит (удаление подозрительного вируса или вредоносного файла из безвредного файла), пользователь может перестать отвечать на предупреждения или выбрать стратегию защиты (разрешить все действия или отключить это действие с помощью антивирусной утилиты). При использовании антивирусных систем, анализирующих поведение программ, всегда есть защищенный компьютер или выполняются команды вирусного кода, которые могут повредить сеть. Чтобы устранить такие ограничения, позже был разработан метод эмуляции (симуляции), который позволяет запускать программу в эксперименте в искусственно созданной (виртуальной) среде, часто называемой песочницей, без возможности повреждения информационной среды. Использование методов анализа поведения программ для обнаружения как известных, так и неизвестных вредоносных программ и их высокой

1.3 Классификации антивирусных программ

Существует несколько классификаций антивирусных программ: по исполнению, по расположению в оперативной памяти и по способу защиты от вирусов.

Антивирусные программы делятся по исполнению (средства блокировки) на:

программное обеспечение;

программное и аппаратное обеспечение.

Благодаря своему расположению в оперативной памяти, он выделяется:

резидентные (они начинают работать при запуске операционной системы, постоянно находятся в памяти компьютера и автоматически проверяют файлы);

нерезидентные (запускаются по запросу пользователя или в соответствии с расписанием для них).

В зависимости от типа защиты от вирусов различают:

Программы обнаружения или сканеры обнаруживают вирусы в оперативной памяти, на внутренних и/или внешних носителях и выводят сообщение при обнаружении вируса.

Медицинские программы (фаги, полифаги) находят зараженные файлы и "обрабатывают" их. Среди таких программ есть полифаги, способные удалять различные типы вирусов, наиболее известными из антивирусных программ являются полифаги Norton AntiVirus, Доктор Веб, Антивирус Касперского.

Программы вакцинации (иммунизаторы) иммунизируют систему (файлы, каталоги), блокируют действие вирусов.

Программы аудита являются наиболее надежными с точки зрения защиты от вирусов. Аудиторы запоминают начальное состояние программ, каталогов и системных областей на диске до тех пор, пока компьютер не будет заражен (обычно на основе контрольных сумм), а затем сравнивают текущее состояние с исходным, отображая обнаруженные изменения на экране.

Программы мониторинга начинают работать после запуска операционной системы, они постоянно хранятся в памяти компьютера и автоматически проверяют файлы по принципу "здесь и сейчас".

Программы фильтрации (sentinels) обнаруживают вирус на ранней стадии, пока он не начнет размножаться. Сторожевые программы - это небольшие резидентные программы, предназначенные для обнаружения действий, специфичных для вирусов.

**ГЛАВА 2. СОЗДАНИЕ АНТИВИРУСА.**

**2.1 Выполнение работы**

В рамках данной работы мы выяснили, что наиболее целесообразно использование программных средств защиты информации, так как они обеспечивают достаточную защиту для ОС. Также, неотъемлемой частью комплекса мер является применение организационных средств защиты информации.

В основу построения системы антивирусной защиты должны быть положены следующие принципы:

1. Принцип реализации единой технической политики при обосновании выбора антивирусных продуктов для различных сегментов локальной сети.
2. Принцип полноты охвата системой антивирусной защиты всех устройств в локальной сети.
3. Принцип непрерывности контроля локальной сети, для своевременного обнаружения компьютерной инфекции.
4. Принцип централизованного управления антивирусной защитой.
5. Принцип ограничения доступа к устройствам по принципу белого листа.

Принцип реализации единой технической политики предусматривает использование во всех сегментах локальной сети только антивирусного ПО, рекомендуемого подразделением антивирусной защиты предприятия. Эта политика носит долгосрочный характер, утверждается руководством предприятия и является основой для целевого и долговременного планирования затрат на приобретение антивирусных программных продуктов и их дальнейшее обновление.

Принцип полноты охвата системой антивирусной защиты локальной сети предусматривает постепенной внедрение в сеть программных средств антивирусной защиты до полного насыщения в сочетании с организационно-режимными мерами защиты информации.

Принцип непрерывности контроля за антивирусным состоянием локальной сети подразумевает такую организацию ее защиты, при которой обеспечивается постоянная возможность отслеживания состояния сети для выявления вирусов.

**2.2 Ход работы.**

Вначале мы долго раздумывали, на каком языке нам написать антивирус, и выбирая из довольно многих, мы остановились на Python, т. к. мы знаем его на очень хорошем уровне. Далее ознакомясь с теорией, узнали основные принципы сканирования, анализа данных и выявления вирусов. Изучили структуру файла, и как достать из него нужную информацию. Для начала мы решили реализовать самый простой метод сканирования - проверка вредоносных хэшей программы на наличие в базе данных. Сразу же нашли приватную базу данных на закрытых источниках, в которой содержится более 30 миллионов вредоносных хэшей, к слову, это в 5 раз больше, чем у всемирно известного антивируса - Dr.Web. После этого мы быстро написал код, который позволяет выбрать нужный файл, взять его хэш, и проверить его на наличие в базе данных, если такой имеется, то файл считается вирусом. Вскоре мы поняли, что этот метод недостаточно хороший, т. к. он может распознать только те вирусы, которые есть в базе данных, при условии, что каждый день создается более 1000 новых вирусов. Поэтому приняли решение сделать универсальный метод, который не будет зависеть ни от чего, и сам сможет определить вирус. Этим методом является создание машинного обучения, анализирующего файл на наличие определенных данных, которые помогут определить, заражен ли файл вирусом или нет. Изучив необходимую информацию, мы сразу приступили к написанию данной программы. После ее завершения мы подумали об удобстве использования антивируса, и решился сделать удобный, понятный, локализированный интерфейс. Для этого мы сначала сделали дизайн программы в Adobe XD, после чего, смотря на созданный макет, мы пытались повторить его, путем написания кода.

**Заключение**

В ходе работы над данным проектом была тщательно проанализирована предметная область антивирусной защиты сетей малых предприятий. Были изучены рекомендованные источники теоретических данных и актуальные предложения передовых вендоров антивирусного программного обеспечения. Было подобрано оптимальное антивирусное решение, совмещающее необходимый функционал.

В ходе исследования предметной области был сформулирован тезис, суть которого заключается в том, что ни один антивирус не способен обеспечить абсолютную защиту информационных систем. Антивирус способен защитить от многих опасностей, но основным источником опасности остаётся конечный пользователь.

Для того чтобы минимизировать угрозу ИС необходимо поддерживать достаточный уровень компьютерной грамотности пользователей и иметь знания поддержания уровня безопасности информационной системы.

Продуктом нашего проекта стала антивирусная программа Spectrum Security.

**Список литературы**

1. [**https://ru.wikipedia.org/wiki/Антивирусная\_программа#:~:text=Антиви́русная%20програ́мма%20(антиви́рус%2C%20средство%20антивирусной,или%20операционной%20системы%20вредоносным%20кодом**](https://ru.wikipedia.org/wiki/Антивирусная_программа#:~:text=Антиви́русная%20програ́мма%20(антиви́рус%2C%20средство%20антивирусной,или%20операционной%20системы%20вредоносным%20кодом)
2. [**https://www.zeluslugi.ru/info-czentr/it-glossary/term-antivirus**](https://www.zeluslugi.ru/info-czentr/it-glossary/term-antivirus)
3. [**https://infourok.ru/individualnyj-proekt-po-discipline-informatika-na-temu-antivirusy-analiz-sovremennyh-antivirusnyh-programm-4374397.html**](https://infourok.ru/individualnyj-proekt-po-discipline-informatika-na-temu-antivirusy-analiz-sovremennyh-antivirusnyh-programm-4374397.html)
4. [**https://kopilkaurokov.ru/informatika/presentacii/proiekt-analiz-biesplatnykh-antivirusnykh-proghramm**](https://kopilkaurokov.ru/informatika/presentacii/proiekt-analiz-biesplatnykh-antivirusnykh-proghramm)

**ПРИЛОЖЕНИЕ**



|  |
| --- |
|  |

|  |
| --- |
|  |

|  |
| --- |
|  |

|  |
| --- |
|  |

|  |
| --- |
|  |