**IT-Колледж “Сириус”**

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

**ДОКЛАД**

по дисциплине “Введение в Специальность”

на тему “Вирусы и Python”

Выполнил:  
Студент группы

1.9.7.1  
Носков Михаил Петрович

Принял:

Старший преподаватель  
Тенигин Альберт Андреевич

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

IT-Колледж “Сириус”  
2022

Оглавление

[1 Введение 3](#_Toc114837377)

[1.1 Вирусы 3](#_Toc114837378)

[1.2 Python 5](#_Toc114837379)

[2 Основная часть 7](#_Toc114837380)

[2.1 Вирусы на Python – это возможно? 7](#_Toc114837381)

[2.2 Вирусы, которые можно написать на Python 8](#_Toc114837382)

[2.3 Самостоятельные попытки создания вирусов 9](#_Toc114837383)

[2.4 Поиск вирусов, используя Python 10](#_Toc114837384)

[3 Вывод 11](#_Toc114837385)

[Список литературы 12](#_Toc114837386)

# 1 Введение

## 1.1 Вирусы

Вирусы – это микроорганизмы, которые являются неклеточными инфекционными агентами, живут, размножаются за счёт клеток другого организма.

Компьютерный вирус – вредоносная программа или код, нарушающий корректную работу компьютера, программ и их компонентов, а также использующий данные, хранящиеся на заражённом ПК в целях создателя вируса без ведома владельца этих данных.

За время существования персональных компьютеров вирусы приобрели разный вид, тип нанесения вреда, а также стали выполнять различные функции. Для борьбы с ними нужно было придумать, как отличать одного от другого, поэтому специалисты данной сферы разработали способ классификации вирусов по основным пунктам: по среде обитания, по степени воздействия, по способам заражения среды обитания и по методам маскировки.

1. Среды обитания – системные области компьютера и его операционной системы или приложения, в которые проникает и встраивается компьютерный вирус.

Различают следующие среды обитания:

* Файловые – это вирусы, которые могут использовать файловую систему для распространения по и на другие ПК
* Загрузочные – это вирусы, которые могут записываться в часть диска, загружающуюся при запуске системы/этого диска
* Сетевые (часто их называют сетевыми червями) – это вирусы, которые используют заражённые протоколы и возможности локальных и глобальных сетей для заражения других устройств.
* Макровирусы – это вирусы, которые используют уязвимости различных программ, которые используют свои макроязыки

1. Степени воздействия – уровень опасности, которую представляет вирус для персонального компьютера

Различают следующие степени воздействия:

* Безвредные (данные вирусы не вредят программному обеспечению или ПК в целом, они просто используют место на накопителях для своего распространения)
* Неопасные (этот тип вирусов не помешает работе персонального компьютера, но его работа будет проявляться в виде звуковых и/или графических “эффектах”)
* Опасные (наносят вред персональному компьютеру)
* Очень опасные (действия данных вирусов могут привести к потере программ, важной информации и целых системных разделов диска)

1. Способы заражения среды обитания – варианты того, как вирус проникает в целевую точку.

Различают следующие виды вирусов по способам заражения:

* Перезаписывающие (эти вирусы удаляют содержимое некоторых файлов, взамен вставляя свой код. Благодаря этому их можно довольно просто вычислить)
* Паразитические (данная разновидность вирусов отличается от предыдущей тем, что они частично или полностью оставляют код заражаемых файлов. Пользователь может не заметить на ранних этапах, но антивирус справится довольно быстро)
* Вирусы-компаньоны (вирус переименовывает оригинальный файл или перемещает его в другое место, а сам создаёт свою копию с начальным названием файла. При запуске выполняется код вируса, а потом код файла)
* Файловые черви (эти вирусы не заражают файлы, распространяясь за счёт копирования и перемещения самих себя в разные директории под привлекающими названиями в надежде, что их кто-нибудь когда-нибудь запустит…)
* Вирусы-ссылки (данный раздел вирусов не меняет физических свойств и содержания файлов, но изменяют необходимые поля файловой системы для выполнения своего кода)

1. Способы маскировки – действия, благодаря которым вирус остаётся незаметным как для пользователя, так и для различных антивирусов.

Различают следующие виды вирусов по способам маскировки:

* Шифрованные (эти вирусы шифруются случайно выбранным ключом и неизменимым шифратором)
* Полиморфные (они постоянно меняют не только ключ, но и алгоритмы шифратора, что осложняет его обнаружение)
* Шифровальщики (делаю всё, чтобы изначально выглядеть как обычные текстовые, графические и прочие файлы)

## 1.2 Python

Python является интерпретируемым высокоуровневым языком программирования, основанным на динамической строгой типизации. Его создателем является Гвидо ван Россум, который начал работу над Python в 1980-ых годах. Когда он выгрузил исходный код языка в феврале 1991 года, мало кто мог предположить, что данное творение уже совсем скоро станет одним из наиболее популярных языков программирования.

Через 9 лет вышел релиз второй версии Python, в которой было добавлено большое количество важных инструментов.

На данный момент времени самой новой версией, доступной пользователям считается версия Python 3.10(.7), вышедшая 4 октября 2021 года, а её самый первый релиз состоялся 3 декабря 2008 года. Тем не менее, многие разработчики связывают свою деятельность с предыдущей версией.

Стоит ли говорить, что за столь большое время развития Python набрал большую аудиторию, в наши дни постоянно являясь одним из трёх лидеров мировых рейтингов по языкам программирования. Сейчас им пользуется около 10 миллионов человек (Рисунок 1). И это не удивительно, ведь у Python есть много плюсов.

Некоторые из них я перечислил далее:

1. Python наиболее оптимален для новичков благодаря простоте и понятности команд на интуитивном уровне. В синтаксисе нет большого количества строжайших правил, а в случае возникновения вопроса любой может обратиться за помощью ко множеству документаций и форумов. К примеру, в сообществе GitHub состоит около 1 миллиона человек.
2. Он является очень многофункциональным языком – под всё есть библиотеки с подробными документациями и водоразборами. Можно писать всё что угодно: от консольных программ до разнообразных компьютерных вирусов.
3. Python является языком программирования с открытым исходным кодом.
4. Обладает кроссплатформенностью, то есть может работать под управлением большинства известных операционных систем.
5. Поддерживает объектно-ориентированное программирование, понятное многим людям.

Рисунок 1 - Статистика языков программирования за август 2022 года

К минусам Python можно отнести то, что Python – некомпилируемый язык (можно отнести как к плюсам, так и к минусам, в зависимости от целей разработчика) и высокую конкуренцию.

# 2 Основная часть

2.1 Вирусы на Python – это возможно?

Для того, чтобы понять, возможно ли создавать вирусы на Python, нужно выяснить, какие функции получится выполнять с помощью него (Рисунок 2).



Рисунок 2 - Те самые возможности…

Для работы нашего вредоносного кода нужно, чтобы он взаимодействовал с файловой системой. Идеальным вариантом для этого является встроенная библиотека OS, которая даёт доступ к:

* запуску команд из консоли (позволит вирусу получить почти неограниченный контроль над персональным компьютером)
* сканированию файловой системы (нужно для обнаружения потенциальных файлов-переносчиков, а также для поиска подключённых переносных накопителей)
* переименованию, созданию, перемещению, удалению, редактированию директорий и файлов (эти возможности помогут нам заражать то, в чём мы найдём уязвимости)

Так же для связи с вирусом можно использовать библиотеку socket, которая позволяет установить удобное подключение по порту, устанавливаемому вручную.

Правда, для написания вирусов Python не подходит тем, что он не компилируется. Единственное, что можно сделать – собрать все используемы скрипты, файлы и библиотеки в самораспаковывающийся архив, чем успешно занимаются некоторые автоматические инструменты, такие как Pyinstaller.

2.2 Вирусы, которые можно написать на Python

Если постараться, то можно написать что угодно, а разнообразие библиотек упростят процесс в разы. Тем не менее, следующие виды вирусов написать на Python будет легче других:

1. BackDoor – это вирус, позволяющий получить удалённый доступ к файлам и управлению операционной системы.

Благодаря вышеупомянутой библиотеке Socket мы можем устанавливать связь с компьютером жертвы

1. KeyLogger – это вирус, позволяющий отслеживать нажатия клавиш на компьютере жертвы. Благодаря этому можно получить скрытые пароли при их вводе. Для этого хорошо подходит библиотека Keyboard, способная не только отслеживать нажатия, но и совершать их.
2. Шифровальщик – это вирус, который шифрует все файлы жертвы, шантажируя её с целью получения выкупа доступа к ним. Как уже говорилось выше, библиотека OS даёт доступ к файлам, их можно открывать, редактировать и сохранять.
3. Вымогатель – это вирус, который блокирует доступ к системе путём открытия провокационных окон. Действует с целью получения выкупа доступа к ней. Библиотека Pygame позволяет открывать окно с размерами, превышающими размеры экрана, отслеживать нажатия горячих клавиш. Их можно будет сбрасывать при помощи библиотеки Keyboard.
4. RAT – BackDoor на максималках с возможностью просмотра экрана.
5. Стиллер – вирус, который получает (крадёт) пароли от конкретных сетей.
6. Вирус-пранк – вирусы, которые созданы с целью поставить человека в неловкое положение, подшутить над ним и т.д. и т.п.

2.3 Самостоятельные попытки создания вирусов

О создании своего собственного компьютерного вируса думал хоть раз в жизни каждый, но не каждый взялся за это трудное занятие. А те немногие, кто брался, в основном построчно копировали чужой код, взятый с постов, гайдов и т.п.

Я уже пробовал создавать многофункциональный вирус, который можно отнести к классу RAT. Изначально в его функции должны были входить только:

* Распространение по USB-накопителям (заражая все файлы, хранящиеся на них, при подключении устройства)
* Получение сохранённых на заражённом устройстве wi-fi паролей и отправка их при помощи библиотеки Socket на мой персональный компьютер

В ходе работы были добавлены следующие функции:

* Дистанционное управление заражёнными устройствами с возможностью просмотра экрана жертвы
* Кража паролей Яндекс

Целевой аудиторией данного вируса были школьные ПК в целях изучения скорости его распространения. Система кибербезопасности в школе была на таком высоком уровне, что при подключении заражённого переносного устройства компьютеры просто выключались. На самом деле, эти ПК были на столько маломощными, что открытие браузера было для них подвиг - не то, что обработать множество команд от вируса.

За время написания кода выяснилось, что самому с нуля без опыта и уже готовых функций создавать вирус бессмысленно и не выгодно, из-за чего проект был свёрнут. В итоге получилось собрать около 20 wi-fi паролей от школьных роутеров и точек доступа неосторожных учеников, вводивших их со школьных ноутбуков. P.S. Все они были мной уничтожены.

## 2.4 Поиск вирусов, с использованием Python

Для обнаружения вирусов нужно знать, чем они отличаются от обычных файлов и системных процессов. К примеру, появление какого-либо нового файла, не являющегося промежуточным результатом работы других надёжных программ, без ведома пользователя будет вызывать подозрение. Появление таковых файлов можно отслеживать при помощи модуля OS, сканируя всю файловую сеть каждые x минут/часов/секунд и т.п.

Также если у вас на ПК выполнилось странное действие (открылось окно, включилась мелодия и т.п.) с файловой системой, то можно отследить, какой именно файл выполнил его. Например, можно написать сканер процессов и активностей на Python, что поможет сузить область поиска зловреда.

Получив список подозрительных файлов, программа будет сравнивать их поведение с найденными до этого вирусами. В случае если сходство является значительным, можно сообщать об этом пользователю.

Такой «борец с вирусами» будет малоэффективен и неудобен в использовании, но, опять же, только для интереса можно заняться его разработкой.

Можно сказать, что Python более подходит под написание вирусов, чем под написание антивирусов.

# 3 Вывод

Написание вирусов на Python – весьма интересное занятие, которое может принести свои плоды в виде новых навыков благодаря тому, что ты находишь выходы из нестандартных ситуаций стандартными библиотеками.

Вирусы на Python обладают многозадачностью, их можно настроить под любую ситуацию. Тем не менее сам процесс их создания весьма трудоёмок и отнимает много времени. Одно дело – написать вирус, другое – спрятать от антивируса или скрыть из диспетчера задач.

Для меня опыт в написании вредоносного кода не столько повысил мои навыки в написании вирусов, сколько дал понять, на сколько простыми паролями мы привыкли защищать свои данные, ведь большинство паролей было из ряда: Vlad-2008; 0987654321; system32; password и т.п., и они все будут легко подобраны при помощи Brute-Force.

# Список литературы

1. Официальный сайт Python - <https://www.python.org>
2. Документации к библиотекам - <https://docs.python-guide.org>
3. Информация о биологических вирусах – Пасечник В.В., Каменский А.Я., Швецов Г.А. Учебник для общеобразовательных учреждений по биологии 8 класс
4. Н. Марков, И. Афанасьев, Т. Бабичева, И. Русанен, В. Паперно, В. Линьков “Python глазами хакера” 2022г.3
5. Статья про антивирус - <https://qna.habr.com/q/485069>