

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**

Федеральное государственное автономное образовательное учреждение

высшего образования

**«Дальневосточный федеральный университет»**

|  |  |
| --- | --- |
|  | **ШКОЛА ЕСТЕСТВЕННЫХ НАУК** |

**Кафедра информационной безопасности**

Пузан Сергей Александрович

|  |
| --- |
| РАЗРАБОТКА ПЛАТФОРМЫ МОНИТОРИНГА И СКАНИРОВАНИЯ ВРЕДОНОСНЫХ ФАЙЛОВ |

**КУРСОВАЯ РАБОТА**

по дисциплине «Защита в операционных системах»

Специальность 10.05.01 «Компьютерная безопасность»

Очной формы обучения

|  |
| --- |
| Студент группы С8117 ммзи \_\_\_\_\_\_\_\_\_  (подпись) |
| Руководитель  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (подпись) (и.о.ф) |
| Регистрационный № \_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  подпись И.О.Фамилия  « \_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2021г. | Оценка \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (подпись) (и.о.ф)  «\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2021г. |

г. Владивосток

2021

Оглавление

[Введение 3](#_Toc12324468)

[1 Обзор литературы 5](#_Toc12324469)

[1.1 Общие сведения о музейных культурах микроорганизмов 5](#_Toc12324470)

[1.2 Основные методы хранения культур микроорганизмов 8](#_Toc12324471)

[1.2.1 Методы непродолжительного хранения микроорганизмов 9](#_Toc12324472)

[1.2.2 Методы продолжительного хранения микроорганизмов 13](#_Toc12324473)

[1.3 Хранение морских микроорганизмов 16](#_Toc12324474)

[2 Материалы и методы 17](#_Toc12324475)

[2.1 Состав сред, используемых в работе 17](#_Toc12324476)

[2.2 Методы хранения культур 18](#_Toc12324477)

[3 Результаты и обсуждение 20](#_Toc12324478)

[Заключение 27](#_Toc12324479)

[Список литературы 28](#_Toc12324480)

# Введение

Любая инфраструктура, реализуемая с использованием информационных технологий, в той или иной степени подвержена угрозе нарушения информационной безопасности, причем атакам злоумышленников подвергаются как компании коммерческого, так и государственного секторов. Зачастую авторы вредоносных программ даже не нацеливают свое ПО против конкретных компаний – их целью является нанесение максимального вреда и придание огласке такого рода происшествий.

Подверженность различных инфраструктур атакам вредоносных программ объясняется не только наличием уязвимостей в используемом ими программном обеспечении (далее – ПО), но и в неправильной или недостаточной его настройке. Распространенным решением по защите компьютерной системы от различных видов вредоносного ПО является использование антивирусных программ, однако ни один антивирусный продукт не может гарантировать абсолютную защиту от вредоносных файлов, так как существует множество способов, позволяющих обходить защитные механизмы антивирусов, отключать их, или же вовсе быть «невидимыми» для их алгоритмов сканирования.

Одним из способов по уменьшению рисков заражения и получению более точных результатов анализа файлов является объединение нескольких технологий в одну платформу. Существуют сервисы, использующие на своей основе практически все известные антивирусные программные модули сканирования, что в конечном счете позволяет проанализировать отчеты о сканировании экземпляра от разных продуктов и сформировать наиболее точный вердикт. Основная проблема, встающая на пути использования подобных сервисов – конфиденциальность данных. В силу различных ограничений многие организации не могут свободно выгружать все имеющиеся у них файлы на проверку.

В связи с этим целью данной работы является разработка платформы для локального мониторинга и анализа экземпляров вредоносных файлов. Для достижения цели поставлены следующие задачи:

1. Изучить виды вредоносных файлов, их свойства;
2. Изучить основные методы анализа файлов;
3. Подготовить системные окружения для ПО, используемого при анализе экземпляров;
4. Разработать программу, реализующую управление задачами по сканированию файлов.

# Методы анализа файлов

Одной из задач авторов вредоносного ПО является его сокрытие от методов анализа, применяемых в антивирусных продуктах. Таким образом, зачастую Анализ вредоносных файлов делится на два этапа – статический и динамический.

* 1. **Статический анализ**

Статический анализ подразумевает под собой исследование программы на наличие вредоносного кода без ее запуска. В него входит поиск необычных для чистых файлов артефактов, строк, ресурсов, чтение дизассемблированного кода программы, проверка хеш-сумм по базам данных, а также эвристический анализ, выполняемый в основном антивирусами. Отдельно стоит пояснить суть эвристического анализа для более полного понимания принципов работы ПО, используемого в данной работе.

Для удобства работы создаем расшаренную папку и запрещаем в ней выполнение любых файлов (будет использоваться для хранения семплов и их сканирования без пересылки на виртуалку).

Антивирус Касперского:

1. Прописать папку с антивирусом в PATH
2. Команда: avp.com SCAN
3. Флаги:
   1. /i0 – выдать только репорт
   2. /RA:<report\_file> - сохранить все события в репорт
   3. /R:<report\_file> - сохранить только критические события

Можно добавить разные функции: скан памяти (/MEMORY), автозагрузка (/STARTUP) и т.д. типа на выбор.

Пример команды: avp.com SCAN "E:\Programs\ubuntu-16.04.7-desktop-amd64.iso" /i0 /RA:brokendick.txt

ESET:

1. Добавляем в PATH
2. Команда: ecls [опции] “имя\_файла”
3. Используем опции:
   1. /log\_file=LOGPATH(задает пользователь в настройках скрипта)
   2. /no\_quarantine – не пихаем в карантин
   3. /adv-heur – расширенная эвристика (разницы не заметил)

Windows Defender:

1. Будем обращаться не из Path, а напрямую через команду “%ProgramFiles%\Windows Defender\MpCmdRun.exe” -Scan -ScanType 3 -DisableRemediation -File “ПУТЬ К ФАЙЛУ”

По всей видимости, придется файл из шары копировать. Антивирусы не горят желанием сканировать проги из нее. Более того, надо запускать все команды от имени администратора.

Как мы запускаем кукушку:

- Из-под рута пишем: /home/cuckoo/cuckoo/bin/cuckoo rooter –sudo –group cuckoo

- Из-под куку-пользователя пишем: . ~/cuckoo/bin/activate и cuckoo –debug

VMCloak.

Чистый образ – win7clean

Клон с надстройками – win7snap

# Список литературы

https://math-it.petrsu.ru/users/semenova/Informatika/DOC/MUM\_65/Lections/Comp\_bez\_Lec.pdf