**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»**

**Факультет безопасности информационных технологий**

**Дисциплина:**

«Технологии и методы программирования»

**ОТЧЕТ ПО ЛАБАРАТОРНОЙ РАБОТЕ №3**

**«“Необходимое” обновление»**

**Выполнили:**

Ливада Е.А., студент группы N33481

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

(подпись)

**Проверил:**

Ищенко А.П.

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

(отметка о выполнении)

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

(подпись)

Санкт-Петербург

2021г.

Содержание

[1 Разработка локальной программы 3](#_Toc86760822)

[1.1 Задание 3](#_Toc86760823)

[1.2 Описание продукта 3](#_Toc86760824)

[1.3 Функционал программы и краткая инструкция 8](#_Toc86760825)

[Заключение 9](#_Toc86760826)

# 1 Разработка локальной программы

**Цель работы:** разработать программу, которая под видом системного обновления собирает информацию о программе, после чего эта информация защищается от любого изменения предварительно зашифровывая все данные.

## Задание

1. Создать текстовый документ (sys.tat), в котором будет содержаться «Системная информация».
2. Написать программу-инсталлятор sys\_doc.exe для этого документа, **которая под видом установки обновления (с отображением строки прогресса обновления) к какой-нибудь программе** (например, Блокнот или Paint):

* Запрашивает у пользователя папку (должен быть вариант использования существующей папки и вариант создания собственной) для копирования «Системной информации».
* Записывает в папку файл с исполняемым кодом программы secur.exe (аналог требований к template.tbl из лабораторной работы №1), защищающей sys.tat.
* Собирает (возможную) информацию о компьютере, на котором устанавливается программа.
* Кодирует эту информацию и записывает в файл sys.tat.
* Подписывает её личным ключом пользователя программы и записывает подпись, например, в реестр Windows в раздел HKEY\_CURRENT\_USER\Software\Фамилия\_студента как значение параметра Signature.
* Запускает secur.exe для защиты sys.tat от несанкционированного доступа.
* Прописывает запуск программы secur.exe при выполнении функции Open для sys.tat, чтобы защита срабатывала и после перезагрузки ОС (есть несколько способов такой «привязки»).

1. В саму программу защиты secur.exe включить следующий функционал:

* Запрос у пользователя информации об имени раздела реестра с электронной цифровой подписью (фамилией студента).
* Считывание подписи из указанного выше раздела реестра, которая проверяется с помощью открытого ключа пользователя.
* Разрешение или запрет просмотра «Системной информации» в файле sys.tat в зависимости от правильности указания ключа.

1. При неудачной проверке работа защищаемой программы должна прекращаться с выдачей соответствующего сообщения.
2. Собираемая о компьютере информация включает в себя как минимум:

* Имя пользователя,
* Имя компьютера,
* Конфигурацию компьютера (память и процессор, как минимум) и версию ОС.

## Описание продукта

Программа написана на языке python с использованием различных библиотек для создания видимости обновления, а также шифрования секретной информации о системе.

При запуске программы не от имени пользователя появится уведомление о недостатке прав у пользователя, это сделано так как системное обновление происходит с доступом администратора.



Рисунок 1 – недостаток прав

Если прав всё же достаточно, программа запустится, предложит выбрать папку для установки обновления. В соответствии с заданием можно выбрать путь к несуществующей папке, она будет создана. Далее начинается установка обновления.

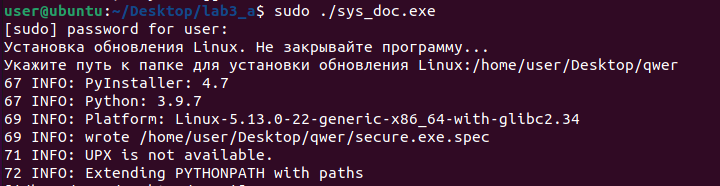


Рисунок 2 – установка обновления

Рассмотрим, что получилось в выбранной папке. В ней образовались два файла: исполняемый файл, защищающий уже зашифрованную информацию о системе.

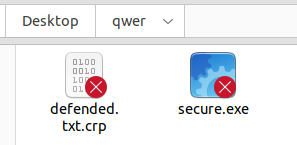


Рисунок 3 – новые файлы в целевой папке

Для разблокировки информации надо запустить исполняемый файл от имени администратора, иначе выйдет ошибка о недостатке прав. В защите присутствует проверка двух значений: имени окружения куда помещался секретный пароль и сам секретный пароль. Оба эти значения находятся внутри исполняемого файла secure.exe в виде хэша md5, такое решение позволяет обезопасить программу от ревёрса. При верно введенных данных программа разблокирует содержимое файлов.

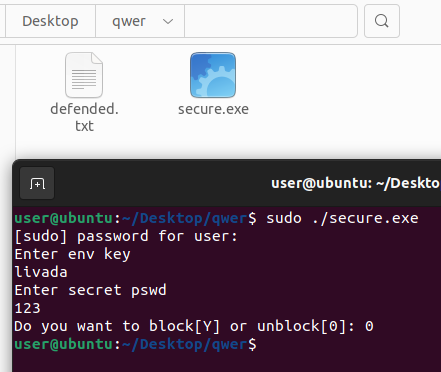


Рисунок 4 – Разблокировка данных

Внутри файла defended.txt содержится вся информация, запрошенная по тз

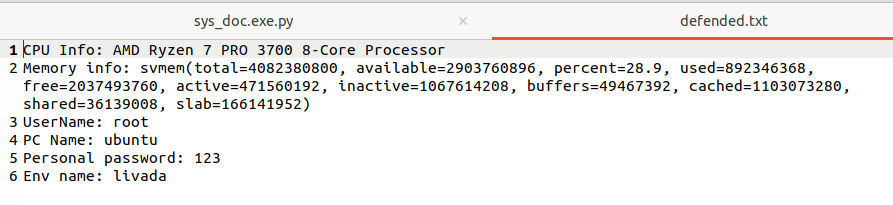


Рисунок 5 – Информация про систему

Используя всё ту же программу secure.exe можно заблокировать все файлы обратно.

Программа secure.exe на самом деле берется из файла sys.tat, который содержит некую зашифрованную информацию. На самом деле, это скрипт на языке python, который впоследствии перекомпилируется в secure.exe с помощью библиотеки PyInstaller, активируя при этом защиту.



Рисунок 6 – Содержимое sys.tat

Таким образом всего из 2 файлов получается выполнить все условия технического задания.

## Функционал программы и краткая инструкция

Данная программа позволяет собирать данные о компьютере-жертве.

Инструкция:

1. Скачать файлы sys\_doc.exe и sys.tat на компьютер жертвы.
2. Используя права администратора установить обновление в любую папку.
3. Для просмотра собранных данных необходимо обладать информацией о коде окружения и секретном пароле, они доступны разработчику (livada; 123). Эти данные вводятся в программе secure.exe, которая находится в папке обновления.
4. При необходимости возобновить защиту повторна запустить программу secure.exe в папке установки обновления.

# Заключение

В ходе выполнения лабораторной работы была разработана программа, которая под видом системного обновления собирает информацию о программе, после чего эта информация защищается от любого изменения предварительно зашифровывая все данные