МИНИСТЕРСТВО ПРОСВЯЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Муниципальное бюджетное общеобразовательное учреждение

«Средняя общеобразовательная школа №64 г. Владивостока»

Разработка программного компонента,

реализующего задачи информационной безопасности

Автор работы:

ученик 8 класса Плотников А.В.

Научный руководитель:

учитель информатики МБОУ «СОШ №64» Руденко Е.О.

г. Владивосток

2023

Оглавление

[Введение 3](#_Toc130127608)

[1. Теоретическая часть 4](#_Toc130127609)

[1.1 Понятие информационной безопасности 4](#_Toc130127610)

[1.2 Использование библиотек в процессе разработки программного обеспечения 5](#_Toc130127611)

[2. Практическая часть 7](#_Toc130127612)

[2.1. Реализация проверки правильности введенного пароля используя условный оператор. 8](#_Toc130127613)

[2.2. Организация самозащиты приложения 8](#_Toc130127614)

[2.3. Описание интерфейса приложения. 9](#_Toc130127615)

[Заключение 12](#_Toc130127616)

[Список литературы 13](#_Toc130127617)

# Введение

Информационная безопасность – практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации.

Один из способов обеспечения информационной безопасности – программное обеспечение, выполняющее функции, которые в той или иной форме обеспечивают безопасность пользователя.

В современном мире информационная безопасность – это жизненно необходимое условие обеспечения интересов человека, общества и государства. Меры по обеспечению информационной безопасности должны осуществляться в разных сферах деятельности человека.

Реальные условия жизни способствовали формированию чрезвычайно широкого и многообразного спектра опасностей и угроз. Многие из опасностей имеют информационную природу либо воздействуют на человека через информационные каналы.

Целью проекта является защита компьютера и хранящейся на нем информации от несанкционированного доступа третьих лиц.

Задачи:

1. изучить основные теоретические и практические аспекты информационной безопасности в части защиты от несанкционированного доступа.
2. создать программный инструмент для защиты рабочего места и информации, хранящейся на нем от несанкционированного доступа.
3. реализовать функционал регистрации инцидента информационной безопасности в случае неуспешной попытки получения доступа к рабочему месту.
4. Теоретическая часть
	1. Понятие информационной безопасности

Под безопасностью информации понимается такое ее состояние, при котором исключается возможность просмотра, изменения или уничтожения информации лицами, не имеющими на это права, а также утечки информации за счет побочных электромагнитных излучений и наводок, специальных устройств перехвата (уничтожения) при передаче между объектами вычислительной техники. Также к информационной безопасности относится защита информации от непреднамеренного уничтожения (технические сбои) [1].

Одним из аспектов информационной безопасности является предотвращение или существенное затруднение несанкционированного доступа к информации (защита информации от несанкционированного доступа), то есть предотвращение доступа к информации третьих лиц.

С целью разработки программного обеспечения для защиты рабочего места от несанкционированного доступа был спроектирован следующий принцип работы, который изображен на Рисунке 1:

* при запуске приложения (приложение может быть добавлено в автозапуск операционной системы), должно инициироваться окно, занимающее весь экран монитора, которое препятствует использованию рабочего места;
* приложение должно блокировать все попытки внештатного завершения работы;
* пользователю рабочего места должна быть доступна функция ввода пароля;
* в случае верного ввода пароля – приложение должно завершать работу для беспрепятственного использования рабочего места и доступа к информации, хранящейся на нем;
* в случае неверного ввода пароля – приложение должно производить фото-фиксацию злоумышленника, и сохранять информацию об инциденте.

Рисунок 1. Описание схемы работы приложения

* 1. Использование библиотек в процессе разработки программного обеспечения

С целью упрощения и ускорения процедуры разработки программного обеспечения можно использовать библиотеки. Библиотека (library) – это наборы подпрограмм, модулей или пакетов, главной задачей которых является упрощение рутинных процессов программирования и поддержка сложных с технической точки зрения проектов.

Библиотеки Python имеют высокий уровень абстракции исходного кода и потенциал метапрограммирования для разработки больших и сложных систем, а также множество библиотек для уникальных функций.

При создании приложения были использованы следующие библиотеки:

1. Tkinter [2]. – встроенная библиотека, предназначенная для создания простых интерфейсов, она была выбрана, так как она очень проста в освоении, а для подобной программы и не требуется более сложных интерфейсов
2. OpenCV [3]. – это библиотека компьютерного зрения, которая предназначена для анализа, классификации и обработки изображений, использовалась для фотографии и с веб-камеры компьютера
3. Практическая часть

С целью создания графического интерфейса приложения и реализации необходимого функционала, с помощью команды import, были подключены необходимые библиотеки, перечисленные на Рисунке 2

Рисунок 2

Для создания основного окна программы и невозможности его закрытия, в соответствии c Рисунком 3 и Рисунком 4, использовался следующий набор команд, позволяющий обеспечить адаптивность интерфейса, для того чтобы независимо от разрешения экрана, программа покрывала весь экран целиком,

Рисунок 3

Рисунок 4

* 1. Реализация проверки правильности введенного пароля используя условный оператор.

Следующая функция, изображенная на Рисунке 5, отвечает за проверку правильности пароля и запуск функции регистрации инцидента информационной безопасности [4]. При вводе пароля, приложение сверяет его с заранее определенным, после чего, если пароль был указан верно, то приложение закрывается, если пароль был указан неверно, происходит фотофиксация пользователя, используя камеру, подключённую к компьютеру, сохранение фотографии в заранее определённый каталог и запись информации о событии в электронный журнал.

 Рисунок 5

* 1. Организация самозащиты приложения

Для того, чтобы ограничить возможность завершения работы приложения используя комбинацию клавиш «alt+f4» была реализована функция [5], изображенная на Рисунке 6.



Рисунок 6

* 1. Описание интерфейса приложения.

Главная задача этого интерфейса – не давать доступ к рабочему столу, и обеспечить возможность ввода пароля. Для этого была реализована функция, изображенная на Рисунке 7, которая открывает программу на весь экран, перекрывая рабочий стол и панель задач.



Рисунок 7

Интерфейс приложения представлен на Рисунке 8.



Рисунок 8

Любая программа, для того чтобы она была интуитивно понятна пользователю, нуждается в базовом обозначении функций. С целью упрощения интерфейса для понимания пользователем, помимо поля ввода, на экране инициализируется текстовое поле, которое информирует пользователя о том, что компьютер заблокирован. Команды, используемые для инициализации элементов управления показаны на Рисунке 9

Рисунок 9

Для того чтобы окно было запущено, требуется набор команд, приведенный на Рисунке 10.



Рисунок 10

Он задает базовые параметры для окна, которые корректируются в зависимости от характеристик компьютера, на котором эта программа была запущена.

Для реализации фотофиксации пользователя при вводе неправильного пароля был использован функционал библиотеки OpenCV [6], приведенный на Рисунке 10.

Рисунок 10

С помощью цикла идет задержка перед выполнением фотофиксации, для того чтобы избежать пересвета и расфокусировки,

После выполнения полученное фото сохраняется в папку «photos», в формате «png».

Таким образом владелец впоследствии сможет просмотреть кто и когда пытался воспользоваться его рабочим местом.

# Заключение

В ходе работы над данным проектом были изучены основные теоретические и практические аспекты информационной безопасности в части защиты от несанкционированного доступа, создан программный инструмент для защиты рабочего места и информации, хранящейся на нем от несанкционированного доступа, реализующий функционал регистрации инцидента информационной безопасности в случае неуспешной попытки получения доступа к рабочему месту и записи информации о нем в журнал.

Таким образом была достигнута цель защиты компьютера и хранящейся на нем информации от несанкционированного доступа третьих лиц.

# Список литературы

1. Информационная безопасность / Текст – электронный // Уральский федеральный университет - URL: https://dpo-rtf.urfu.ru/protect-information/ (дата обращения: 24.02.2023). – Режим доступа: свободный.
2. Докуменация Tkinter / Текст – электронный // сайт по программировании METANIT.COM - 26.09.2022 - URL: <https://metanit.com/python/tkinter/> (дата обращения: 4.03.2023). – Режим доступа: свободный.
3. Документация OpenCV / Текст – электронный // Официальный сайт разработчика библиотеки opencv.org - URL: <https://docs.opencv.org/4.x/d6/d00/tutorial_py_root.html> (дата обращения: 8.03.2023). – Режим доступа: свободный.
4. Майкл Доусон «Программируем на Python» / Майкл Доусон: Питер, 2020. - 42 с.
5. Докуменция PyAutoGui / Текст – электронный // Официальный сайт библиотеки PyAutoGui - URL: <https://pyautogui.readthedocs.io/> (дата обращения: 11.03.2023). – Режим доступа: свободный.
6. StackOverflow / Текст – электронный // Информационный портал stackoverflow.com - 17.09.2017 - URL: <https://ru.stackoverflow.com/questions/702657/> (дата обращения: 13.03.2023). – Режим доступа: свободный.