**Министерство науки и высшего образования Российской Федерации**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
**НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО**

**Факультет безопасности информационных технологий**

**Дисциплина:**

«Технологии и методы программирования»

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №1**

«Локальная и веб-защита»

**Выполнили:**

Бардышев Артём Антонович,

студент группы N3346

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

(подпись)

**Проверил:**

Ищенко Алексей Петрович,

преподаватель, ФБИТ

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

(отметка о выполнении)

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

(подпись)

Содержание

[Введение 3](#_Toc209462830)

[1 ЗАДАНИЕ 1(А): ЛОКАЛЬНАЯ ПРОГРАММА 4](#_Toc209462831)

[1.1 Задание 4](#_Toc209462832)

[1.2 Инструкция по применению 4](#_Toc209462833)

[1.2.1 Первоначальная настройка 4](#_Toc209462834)

[1.2.2 Использование 4](#_Toc209462835)

[2 ЗАДАНИЕ 1(Б): ВЕБ-СКРИПТ 5](#_Toc209462836)

[2.1 Задание 5](#_Toc209462837)

[2.2 Методы защиты контента на веб-страницах 5](#_Toc209462838)

[2.3 Практическая реализация 6](#_Toc209462839)

[Заключение 7](#_Toc209462840)

[Список использованных источников 8](#_Toc209462841)

Введение

Цель работы – разработка и исследование механизмов защиты данных на уровне файловой системы и веб-страниц.

Для достижения поставленной цели необходимо решить следующие задачи:

* локальную программу для защиты файлов в каталоге с управлением доступом и паролем;
* веб-скрипт для ограничения копирования и сохранения контента страниц с возможностью печати и отключением по паролю.

# ЗАДАНИЕ 1(А): ЛОКАЛЬНАЯ ПРОГРАММА

## Задание

Разработать программу для ОС Windows, которая запрещает создание, копирование, удаление или переименование файлов с заданными именами или по маске. Список шаблонов должен храниться в текстовом файле template.tbl. Необходимо обеспечить защиту этого файла от несанкционированного доступа. Отключение защиты должно производиться по паролю, хеш которого хранится в файле template.tbl. Программа должна поддерживать режимы включения и выключения защиты.

## Инструкция по применению

Программа представляет собой единый исполняемый файл lab1a.exe, который может работать в двух режимах. Для работы требуются права администратора.

### Первоначальная настройка

Поместите protector.exe в защищаемый каталог.

1. Запустите командную строку (cmd.exe) в этом каталоге.
2. Выполните команду: lab1a.exe.
3. Программа запросит создание и подтверждение пароля.
4. В каталоге будет создан файл template.tbl, в который необходимо внести маски защищаемых файлов (например, \*.docx, secret.txt). По умолчанию программа будет защищать весь каталог целиком.

### Использование

**Графический интерфейс (GUI):** Запускается двойным щелчком по protector.exe. Позволяет наглядно видеть статус защиты и слежения, а также включать и выключать их с помощью кнопок.

# ЗАДАНИЕ 1(Б): ВЕБ-СКРИПТ

## Задание

Реализовать JavaScript, встраиваемый в HTML-документ, для защиты контента от копирования (выделение, буфер обмена, скриншоты) и сохранения. При этом должна сохраняться возможность печати страницы. Отключение скрипта должно выполняться по паролю, хеш которого хранится в самом скрипте.

## Методы защиты контента на веб-страницах

Защита контента на стороне клиента (в браузере) является комплексной задачей и реализуется комбинацией технологий:

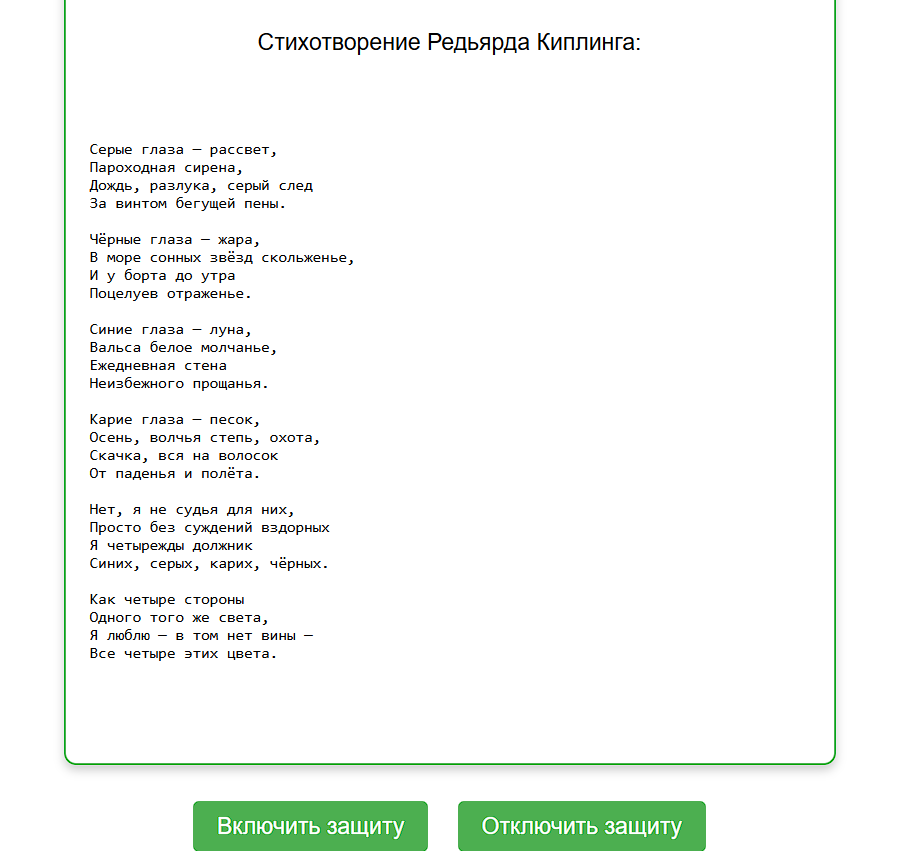
− **CSS** (Cascading Style Sheets): Свойство user-select: none; запрещает пользователю выделять текст на странице.

− **JavaScript** (DOM Events): Перехват событий мыши и клавиатуры позволяет блокировать стандартные действия. Например, отмена действия по умолчанию для события contextmenu блокирует вызов контекстного меню (правый клик), а для keydown – комбинации клавиш (Ctrl+C, Ctrl+S).

− **Web Crypto API**: Современный стандарт для выполнения криптографических операций в браузере. Используется для безопасного сравнения паролей: введенный пользователем пароль хешируется с помощью crypto.subtle.digest() и сравнивается с эталонным хешем, хранящимся в коде.

− **CSS Media Queries**: Правило @media print позволяет применять стили, которые активны только при печати документа. Это используется для скрытия защитных элементов (например, водяных знаков) с печатной версии страницы.

## Практическая реализация

Создадим HTML-документ, для реализации защиты

Заключение

В ходе выполнения лабораторной работы были успешно разработаны и протестированы два программных продукта, решающих поставленные задачи по защите информации.

Это позволило получить и закрепить навыки работы с механизмами безопасности ОС, управления правами доступа, хеширования и хранения паролей, а также применения средств HTML, CSS и JavaScript для защиты клиентского контента.

Список использованных источников

1. Dhikhi, T., Saravanan, M.S. An enhanced intelligent intrusion detection system using machine learning : научная статья. – Текст : электронный. – 2019. – URL : <https://www.ijitee.org/wp-content/uploads/papers/v8i9/H6932068819.pdf> (дата обращения: 10.12.2020).
2. Инфосистемы Джет. «Инфосистемы Джет» выпустила новый обзор решений Anti-APT : сайт. – Текст : электронный. – 2020. – URL : <https://jet.su/about/news/19776/> (дата обращения: 09.05.2021) – Загл. с экрана.
3. Anti-Malware. Защита от целевых атак : онлайн-конференция. – 2021. – URL : <https://www.anti-malware.ru/event/2021/03/30> (дата обращения: 30.03.2021).