МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение высшего образования

«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ   
АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ»

КАФЕДРА ИНФОРМАЦИОННО-СЕТЕВЫХ ТЕХНОЛОГИЙ

КУРСОВОЙ ПРОЕКТ (РАБОТА)  
ЗАЩИЩЕНА С ОЦЕНКОЙ

РУКОВОДИТЕЛЬ

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| профессор, канд. техн. наук |  |  |  | С.Г. Фомичева |
| должность, уч. степень, звание |  | подпись, дата |  | инициалы, фамилия |

|  |
| --- |
| ПОЯСНИТЕЛЬНАЯ ЗАПИСКА К КУРСОВОМУ ПРОЕКТУ |
| РАЗРАБОТКА ПРОГРАММЫ ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО КОПИРОВАНИЯ СО СЪЁМНЫХ НОСИТЕЛЕЙ |
| по дисциплине: ТЕХНОЛОГИИ ПРОГРАММИРОВАНИЯ |
|  |
|  |

РАБОТУ ВЫПОЛНИЛ

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| СТУДЕНТ ГР. № | 3136 |  |  |  | В.А. Панчук |
|  |  |  | подпись, дата |  | инициалы, фамилия |

Санкт-Петербург 2023

**СОДЕРЖАНИЕ**

[ВВЕДЕНИЕ 3](#_Toc149680119)

[1. Назначение и цели создания проекта 5](#_Toc149680120)

[2. Формализация задачи 7](#_Toc149680121)

[2.1. Уникальный идентификатор 7](#_Toc149680124)

[2.2. Хранение списка 9](#_Toc149680125)

[2.3. Мониторинг и аудит 9](#_Toc149680126)

[2.4. Выбор ЯП для программы 10](#_Toc149680127)

[2.5. Кроссплатформенность 9](#_Toc149680128)

[2.6. Визуализация 9](#_Toc149680129)

[2.7. Автозагрузка и запрет на снятие задачи 10](#_Toc149680130)

# ВВЕДЕНИЕ

В современную цифровую эпоху, когда информация распространяется со скоростью света, а данные передаются без особых усилий, важность защиты конфиденциальной информации приобретает первостепенное значение. Разработка программы для защиты от несанкционированного копирования со съемных носителей является важнейшим направлением в области систем предотвращения потери данных (DLP). Данный проект направлен на решение проблемы несанкционированного доступа и утечки данных и представляет собой надежное решение для защиты ценных активов.

Чтобы оценить значимость этого проекта, давайте вкратце познакомимся с историей. На протяжении всего времени человечество стремилось сохранить свои знания и секреты в безопасности, применяя различные методы защиты. Начиная с древних цивилизаций, использовавших методы шифрования для передачи конфиденциальных сообщений, и заканчивая разработкой замков и ключей в эпоху промышленной революции, потребность в безопасной связи всегда была присуща нашему обществу.

Мы переносимся в современную эпоху, когда информация не только ценна, но и уязвима. С экспоненциальным ростом объемов цифровых хранилищ и широким распространением съемных носителей угроза несанкционированного копирования и утечки данных достигла беспрецедентного уровня. Киберпреступники и инсайдеры теперь обладают всеми возможностями для использования уязвимостей, что ставит под угрозу конфиденциальность конфиденциальных данных.

Именно на этом фоне разработка программы для защиты от несанкционированного копирования со съемных носителей приобретает актуальность в современных условиях. Организации различных отраслей, таких как финансы, здравоохранение, технологии, постоянно сталкиваются с риском кражи интеллектуальной собственности, утечки данных и потери доверия потребителей. При отсутствии адекватных механизмов защиты возможные последствия могут быть катастрофическими как в финансовом, так и в репутационном плане.

Внедрение надежной программы защиты от несанкционированного копирования со съемных носителей, позволяет предприятиям активно защищать критически важную информацию, снижая риски, связанные с несанкционированным извлечением данных. Будь то предотвращение копирования конфиденциальных файлов клиентов на незащищенные USB-накопители или мониторинг и контроль передачи конфиденциальных данных на внешние устройства хранения, такая программа обеспечивает эффективную защиту от несанкционированного копирования.

В заключение следует отметить, что разработка программы для защиты от несанкционированного копирования со съемных носителей информации является чрезвычайно актуальной в условиях современного цифрового ландшафта. Удовлетворяя насущную потребность в защите данных в DLP-системах, данный проект призван предоставить организациям комплексное решение для борьбы с постоянно растущими угрозами, связанными с несанкционированным копированием данных. С каждым днем последствия утечек данных становятся все более серьезными, поэтому инвестиции в надежные механизмы защиты становятся обязательным условием для компаний, стремящихся сохранить свои ценные активы и доверие заинтересованных сторон.

# Назначение и цели создания проекта

Целью создания программы для защиты от несанкционированного копирования со съемных носителей, таких как USB-накопители, внешние жесткие диски и карты памяти, является обеспечение защиты конфиденциальной информации, хранящейся на съемных носителях, и предотвращение несанкционированного доступа или утечки данных. Распишем подробнее каждую из всевозможных целей и задач.

* Ведение белых списков разрешенных носителей. Основное назначение программы - создание "белого списка" одобренных или разрешенных съемных носителей. Она позволяет системным администраторам или пользователям создать список определенных USB-накопителей, внешних жестких дисков или других типов съемных носителей, которые разрешены для использования в среде. Любое устройство, не включенное в "белый список", будет заблокировано и не сможет выполнять операции передачи данных.
* Предотвращение утечки данных. Задачей программы является предотвращение несанкционированного копирования или утечки конфиденциальной информации со съемных носителей. Это достигается путем мониторинга и контроля передачи данных на носители и с них. Это позволяет обеспечить доступ к данным и их копирование только авторизованными лицами или системами, что снижает риск утечки данных или кражи интеллектуальной собственности.
* Защита от вредоносного ПО. Ключевым преимуществом программы является ее способность защищать от внедрения вредоносного ПО через вредоносные или зараженные съемные носители. Она обеспечивает взаимодействие с системой только доверенных и авторизованных носителей, что снижает риск проникновения вредоносного ПО, потери или несанкционированного извлечения данных.
* Упрощенный мониторинг и управление. Программа упрощает мониторинг и управление системой за счет централизованного ведения списка авторизованных съемных носителей. Системные администраторы могут легко просматривать и обновлять белый список, предоставляя или отменяя доступ к определенным устройствам в соответствии с требованиями пользователей или политиками безопасности. Это помогает поддерживать контролируемую и безопасную среду, снижая сложность мониторинга огромного количества потенциальных носителей.
* Обнаружение инцидентов. Программа может предоставлять комплексные возможности по обнаружению инцидентов и созданию отчетов о них. Любая попытка доступа или копирования данных с неавторизованных носителей будет регистрироваться и записываться. Это позволяет выявлять потенциальные нарушения безопасности, расследовать инциденты и принимать соответствующие меры по снижению рисков.

Программный проект должен осуществлять:

− ввод данных с клавиатуры и из файла;

− вывод данных на экран, на принтер, в файл;

− защита приложения от неквалифицированных действий пользователя.

# Формализация задачи

Чтобы частично решить проблему несанкционированного копирования со съемных носителей необходимо разработать "белые списки". Создание таких списков предполагает составление перечней разрешенных съемных устройств, что позволяет строго контролировать доступ к системе. Эта стратегия основана на предварительной идентификации и авторизации съемных устройств, чтобы только разрешенные устройства имели возможность взаимодействовать с системой и выполнять операции копирования данных.

Создание "белых списков" можно реализовать путем назначения уникальных идентификаторов разрешенным устройствам и сохранения их в централизованной базе данных или конфигурационных файлах. При подключении съемного устройства программа проверяет его идентификатор среди записей "белого списка". Если идентификатор найден и совпадает с разрешенными значениями, устройству предоставляется доступ, в противном случае оно отклоняется и лишается возможности копирования данных с системы.

Рассмотрим методы реализаций каждого из пунктов по отдельности:



## Уникальный идентификатор

Существуют различные способы проверки подлинности носителя информации с целью защиты от несанкционированного копирования для программы, использующей белые списки. Вот два подхода, которые мы рассмотрим:

1. Аппаратная идентификация. Использовать аппаратные идентификаторы, встроенные в сам съемный носитель, например, уникальные серийные номера или идентификационные чипы. Этот метод проверки подлинности имеет свои достоинства:

* Надежная идентификация: аппаратная идентификация, как правило, уникальна для каждого устройства, что делает ее надежной. Это позволяет свести к минимуму риск подмены или обхода процесса аутентификации.
* Простота реализации: аппаратная идентификация проста в реализации, так как уже реализована в необходимых аппаратных компонентах.

1. Цифровые подписи. Генерирование цифровых подписей для съемных носителей с использованием криптографических технологий. Программа может проверить целостность и подлинность носителя путем проверки цифровой подписи. У этого метода имеются свои плюсы и недостатки.

Плюсы:

* Быстрая и удобная аутентификация: использование подписи, в которой можно сохранить имя и фамилию человека, позволяет идентифицировать устройство без необходимости проверки в белых списках.
* Гибкость и масштабируемость: в отличие от аппаратной идентификации, цифровые подписи не привязаны к конкретным аппаратным компонентам. Они могут быть применены к любому цифровому файлу или носителю, что делает их более гибкими и масштабируемыми для различных устройств и платформ.

Минусы:

* Зависимость от закрытых ключей: цифровые подписи опираются на пару криптографических ключей: закрытый ключ и соответствующий ему открытый ключ. Безопасность системы в значительной степени зависит от сохранности закрытого ключа. Если закрытый ключ будет скомпрометирован, это может привести к несанкционированному доступу или подделке съемного носителя.
* Сложность реализации: Реализация цифровой подписи может быть более сложной по сравнению с аппаратной идентификацией. Она требует создания инфраструктуры открытых ключей (PKI), генерации и управления парами ключей, а также интеграции криптографических алгоритмов в программу "белых списков".

Исходя из сравнения этих двух способов можно сделать вывод, что лучше использовать сразу два метода. В таком случае исключается недостаток закрытого ключа, так как при проверке нужно будет использовать и аппаратный идентификатор, что позволит в любом случае идентифицировать пользователя.

Но в данном проекте можно обойтись и лишь аппаратной идентификацией.

## Хранение списка

Для эффективного управления и ведения белых списков будем использовать реляционную базу данных PostgreSQL. Данное решение обеспечивает большое количество достоинств: целостность и надежность данных, гибкость, расширяемость, безопасность, производительность и масштабируемость.

## Мониторинг и аудит

Мониторинг и аудит каждого входа пользователя в систему является важнейшим аспектом программы защиты. Отслеживание и анализ входов пользователей в систему позволяет выявлять попытки несанкционированного доступа и обеспечивать ответственность в системе. Для реализации этой функции требуется использовать реляционную базу данных и программу, вводящую/выводящую эти данные.

## Кроссплатформенность

## Визуализация

## Выбор ЯП для программы

## Автозагрузка и запрет на снятие задачи