СОДЕРЖАНИЕ

[ВВЕДЕНИЕ 3](#_Toc138014582)

[ГЛАВА 1 ОПИСАНИЕ ПРЕДМЕТНОЙ ОБЛАСТИ 4](#_Toc138014583)

[1.1 Системный реестр Windows 4](#_Toc138014584)

[1.2 Использование системного реестра для ограничения доступа к файлам и папкам 5](#_Toc138014585)

[1.3 Методы защиты доступа в системном реестре Windows 6](#_Toc138014586)

[1.4 Анализ существующих решений. 7](#_Toc138014587)

[WinLock 9](#_Toc138014588)

[WinGuard 10](#_Toc138014589)

[Advanced Folder Encryption 11](#_Toc138014590)

[Deskman 12](#_Toc138014591)

[Выводы 13](#_Toc138014592)

[ГЛАВА 2 РАЗРАБОТКА ПРОГРАММНОГО СРЕДСТВА 14](#_Toc138014593)

[2.1 Выбор программного обеспечения 14](#_Toc138014594)

[2.2 Планирование информационной безопасности 15](#_Toc138014595)

[2.3 Разработка интерфейса программного средства 16](#_Toc138014596)

[ЗАКЛЮЧЕНИЕ 21](#_Toc138014597)

[СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 22](#_Toc138014598)

[ПРИЛОЖЕНИЕ А 23](#_Toc138014599)

# ВВЕДЕНИЕ

С каждым годом информационные технологии занимают все большую роль в жизни людей и организаций.

Широкое распространение компьютеров и интернета приводят к необходимости обеспечения безопасности хранения и передачи данных. Одной из важнейших задач является защита доступа к файлам и папкам на компьютере. Windows – самая распространенная операционная система на персональных компьютерах. Вместе с тем, это делает ее одной из самых уязвимых к атакам злоумышленников. Один из способов обеспечения безопасности — это ограничение доступа к файлам и папкам. Для этого можно использовать системный реестр операционной системы Windows.

Цель данной курсовой работы – рассмотреть методы защиты доступа к файлам и папкам через системный реестр Windows.

Основной задачей является изучение механизмов доступа к файлам и папкам, предоставляемых операционной системой Windows, и исследование возможностей и ограничений использования системного реестра в качестве инструмента защиты.

В качестве теоретической базы используются материалы по безопасности операционных систем и работе с реестром Windows. Результаты работы могут быть использованы системными администраторами и обычными пользователями для обеспечения безопасности своих данных на компьютере.

# ГЛАВА 1 ОПИСАНИЕ ПРЕДМЕТНОЙ ОБЛАСТИ

Защита доступа к файлам и папкам является одной из важных задач в операционной системе Windows. В зависимости от прав доступа, установленных на файл или папку, пользователи могут иметь различные уровни доступа к ним. В системе Windows права доступа на файлы и папки управляются через систему разрешений NTFS (New Technology File System), которая позволяет определить, кто и как может использовать файлы и папки в системе. Разрешения NTFS содержат информацию о создании, чтении, изменении и удалении файлов и папок. Система разрешений NTFS позволяет определить следующие уровни доступа к файлам и папкам:

* Чтение - позволяет просматривать содержимое файла или папки.
* Запись - позволяет изменять содержимое файла или папки.
* Выполнение - позволяет запускать файлы с расширением «exe» или «bat» и выполнять скрипты.
* Полный доступ - позволяет выполнять все действия (чтение, запись и выполнение) с файлами и папками.

Для управления доступом к файлам и папкам в Windows используется системный реестр, который содержит настройки операционной системы и приложений. Изменение значений в системном реестре может повлиять на работу всей системы, поэтому необходимо быть очень осторожным при его изменении. Это особенно верно, когда речь идет о настройке прав доступа к файлам и папкам. Системный реестр Windows представляет собой иерархически организованную базу данных, каждый ключ в которой имеет свои свойства и значения. Как правило, изменение значений в системном реестре производится с помощью специальных инструментов, таких как редактор реестра (regedit.exe) или групповые политики (gpedit.msc).

## 1.1 Системный реестр Windows

Системный реестр Windows — это база данных, которая содержит в себе информацию о конфигурации операционной системы, установленных на компьютере приложениях и сервисах. Реестр является одним из важных  
компонентов операционной системы Windows и используется для совместного доступа к разным типам информации.

Реестр Windows функционирует как централизованный хранилище данных, содержащий информацию, которая периодически используется приложениями и операционной системой для определения настроек, интерфейса и исполнения программных задач. Реестр можно представить в виде древовидной структуры, где узлы являются различными разделами, а листья - ключами и значениями.

Реестр Windows работает следующим образом: при запуске операционной системы загружается ядро (с ядра начинается работа всей операционной системы), инициализируется реестр файлами, хранящимся на жестком диске, и копируется в оперативную память в качестве дерева. После того как реестр загружен в оперативную память, все программы и службы могут получить доступ к его функциональности.

Данные в реестре хранятся в виде ключей и значений. Ключи представляют собой контейнеры для значений, которые хранятся в них. Поиск ключей и значений в реестре Windows может быть выполнен с помощью редактора реестра, который включен в стандартный набор программного обеспечения операционной системы.

Однако, доступ к системному реестру должен быть ограничен, чтобы предотвратить ошибки и утечки информации. Для этого в Windows есть система прав доступа, которая определяет, кто может просматривать или изменять информацию в реестре. Таким образом, злоумышленники не смогут легко изменить настройки системы и нанести вред компьютеру.

Защита доступа к файлам и папкам через системный реестр Windows является одним из методов защиты компьютера. С помощью настройки прав доступа и изменения значений в реестре можно ограничивать доступ  
к информации на компьютере. Однако, важно учитывать, что ошибочно измененные настройки могут привести к неправильной работе компьютера, поэтому использование данного метода должно быть осуществлено с осторожностью.

## 1.2 Использование системного реестра для ограничения доступа к файлам и папкам

Системный реестр Windows предоставляет возможность ограничивать доступ к файлам и папкам через редактирование ключей в реестре. Это может быть полезно, например, если нужно запретить доступ к определенным системным файлам или папкам, чтобы предотвратить несанкционированный доступ или изменение системных настроек.

Для того чтобы ограничить доступ к файлам или папкам через системный реестр, нужно выполнить следующие шаги:

1. Открыть редактор реестра, нажав клавиши Win + R и введя regedit в поле запуска.
2. Найти ключ в реестре, соответствующий файлу или папке, доступ к которому нужно ограничить. Ключи в реестре обычно находятся в разделе HKEY\_LOCAL\_MACHINE или HKEY\_CURRENT\_USER.
3. . Добавить новый ключ в найденном разделе, нажав правой кнопкой мыши на раздел и выбрав New -> Key.
4. Назначить созданному ключу значение, нажав на него правой кнопкой мыши и выбрав New -> DWORD (32-bit) Value.
5. Дать название новому значению, например, AccessDenied.
6. Установить значение 1 для созданного ключа, чтобы запретить доступ к файлу или папке. Для этого нужно дважды щелкнуть на значении, выбрать Decimal и ввести 1 в поле Value data.

После выполнения этих шагов доступ к файлу или папке будет ограничен для всех пользователей на компьютере, включая администраторов. Чтобы убрать ограничение доступа, нужно удалить созданные ключи в реестре.

Важно понимать, что использование системного реестра для ограничения доступа к файлам и папкам может быть опасным, если вы не знаете, что делаете. Неправильная редактирование реестра может привести к сбоям в работе компьютера, поэтому перед выполнением каких-либо изменений важно сохранить резервную копию реестра и следовать инструкциям с осторожностью.

## 1.3 Методы защиты доступа в системном реестре Windows

Защита доступа к системному реестру Windows является важной задачей для обеспечения безопасности операционной системы и сохранения целостности реестра. Существует несколько методов защиты доступа к системному реестру Windows, которые можно использовать для обеспечения безопасности и защиты конфиденциальных данных.

**ACL**

Один из методов защиты доступа к системному реестру Windows — это использование списков контроля доступа (ACL). ACL — это набор правил, которые определяют, какие пользователи и группы имеют доступ к объекту или ресурсу. В системном реестре Windows ACL используется для установки прав доступа к ключам реестра и их значениям.

С использованием ACL можно установить следующие права доступа к ключам и значениям реестра:

* Полный контроль - разрешает чтение, запись и выполнение операций с ключами или значениями реестра.
* Чтение - разрешает только чтение ключей или значений реестра.
* Запись - разрешает только запись ключей или значений реестра.
* Изменение прав - разрешает изменение прав доступа к ключам или значениям реестра.

**Установка прав через политики безопасности**

Другой метод защиты доступа к системному реестру Windows — это установка прав доступа через политики безопасности. Политики безопасности — это набор правил, определяющих, как система должна обрабатывать запросы на доступ к ресурсам. В Windows политики безопасности можно использовать для установки прав доступа к системному реестру.

Существует несколько групп политик безопасности, которые можно использовать для установки прав доступа к системному реестру Windows:

* Политики безопасности локальной машины - эти политики применяются к локальной машине и позволяют управлять правами доступа для всех пользователей и групп на данной машине.
* Политики безопасности домена - эти политики управляют правами доступа к системному реестру для пользователей и групп в пределах домена.
* Политики безопасности организации - эти политики позволяют управлять правами доступа к системному реестру для пользователей и групп в пределах организации.

**Объекты Group Policy**

Объекты Group Policy (GPO) — это контейнеры, которые содержат набор правил для управления настройками компьютера или пользователя. GPO можно использовать для установки прав доступа к системному реестру Windows. Для этого необходимо настроить параметры GPO, связанные с правами доступа к ключам и значениям реестра.

GPO можно установить для определенных пользователей, групп или компьютеров. Кроме того, GPO можно использовать для установки прав доступа к реестру на локальной машине или на уровне домена.

**Диспетчер защиты**

Windows также предоставляет Диспетчер защиты, который можно использовать для установки прав доступа к системному реестру. Диспетчер защиты позволяет с легкостью устанавливать права доступа для конкретных пользователей и групп на различных уровнях реестра.

Кроме того, Диспетчер защиты позволяет создавать новые правила безопасности для ключей и значений реестра и изменять существующие правила доступа. Диспетчер защиты позволяет просматривать текущие правила безопасности для всех ключей и значений реестра, а также просматривать список пользователей и групп и их уровень доступа.

**Резервное копирование и восстановление системного реестра**

Каким бы надежным не был метод защиты доступа к системному реестру Windows, все равно существует риск его повреждения или потери. Для защиты от подобного риска Windows предоставляет возможность создать резервную копию системного реестра. Резервная копия системного реестра является точной копией реестра, которую можно использовать для восстановления системы в случае его повреждения или потери.

При потере или повреждении системного реестра можно использовать резервную копию для восстановления данных и установки новых прав доступа к системному реестру. Помимо этого, резервное копирование системного реестра является обязательным для обеспечения безопасности и сохранности данных операционной системы Windows.

## 1.4 Анализ существующих решений.

Несмотря на то, что в составе Windows есть инструменты для ограничения доступа, на практике оказывается, что они не слишком удобны, причем в самых заурядных ситуациях. Достаточно упомянуть такие простые примеры, как установка пароля на директорию или запрет на открытие Панели управления.

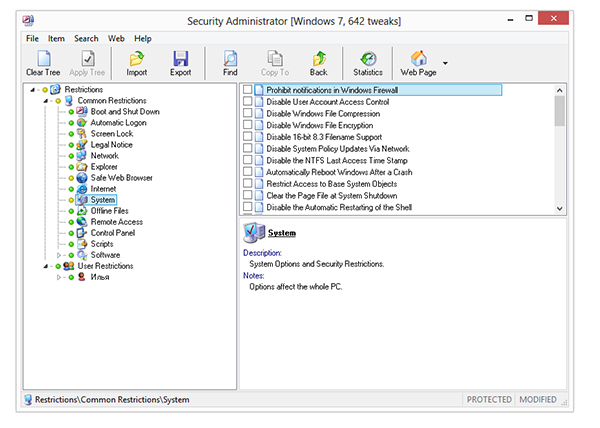
Можно отметить, что в Windows 8, по сравнению с предшествующей ей Windows 7, был усовершенствован родительский контроль. Сейчас с ним можно ознакомиться в разделе «Семейная безопасность» Панели управления. Фильтр имеет следующие возможности:

* Фильтрация посещения веб-сайтов
* Ограничения по времени
* Ограничения на Магазин Windows и игры
* Ограничения на приложения
* Просмотр статистики активности пользователей

Из перечисленного ясно, что даже эти функции помогут администратору компьютера решить многие частные моменты. Поэтому далее пойдет речь о небольших программах, которые позволяют ограничить доступ к информации и системным разделам в дополнение к стандартным инструментам управления ОС Windows.

**Security Administrator**

Рисунок 1.

Security Administrator [](https://www.ixbt.com/soft/images/security-tweaks/1.png)

Программа Security Administrator напоминает типичный системный твикер, но только с акцентом на системную безопасность. Каждая из опций отвечает за определенное ограничение, поэтому общее древо настроек так и называется — «Restrictions». Оно делится на 2 раздела: общие (Common Restrictions) и пользовательские ограничения (User Restrictions).

В первой секции — параметры и подразделы, которые касаются всех пользователей системы. К ним относятся загрузка и вход в систему, сеть, Проводник, собственно Интернет, система, Панель управления и другие. Условно их можно разделить на ограничения онлайн- и офлайн-доступа, но разработчики особо сложной разбивки по вкладкам не рассмотрели. По сути, достаточно и того, что каждый «твик» имеет описание: какое влияние на безопасность оказывает та или иная опция.

Во втором разделе, User Restrictions, можно настроить доступ для каждого пользователя Windows индивидуально. В список ограничений входят разделы Панели управления, элементы интерфейса, кнопки, горячие клавиши, съемные носители и др.

Предусмотрен экспорт настроек в отдельный файл, чтобы его можно было применить, например, на других системных конфигурациях. В программу встроен агент для слежения за активностью пользователей. Файлы журнала помогут администратору проследить потенциально опасные действия пользователя и принять соответствующие решения. Доступ к Security Administrator можно защитить паролем — в далее рассматриваемых программах это опция также имеется де факто.

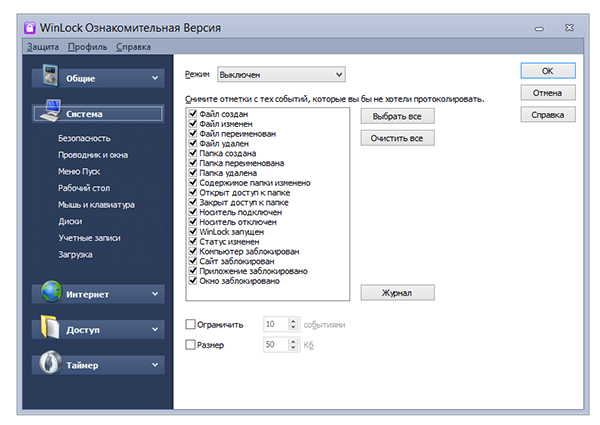
Из недостатков — небольшой список программ, для которых можно применить ограничения: Media Player, MS Office и т. п. Популярных и потенциально опасных приложений намного больше. Усложняет работу отсутствие актуальной для Windows 8 версии и локализации — это как раз тот вариант, когда сложно обходиться без начальных знаний английского.

Таким образом, программа предназначена как для ограничения доступа, так и для гибкой настройки параметров безопасности ОС.

## WinLock

Рисунок 2.

WinLock

[](https://www.ixbt.com/soft/images/security-tweaks/2.png)

В WinLock нет распределения настроек на общие и пользовательские, вместо этого имеются разделы «Общие», «Система», «Интернет». В сумме, возможностей меньше, чем предлагает Security Administrator, но такая логика делает работу с программой более удобной.

К системным настройкам относятся ограничения элементов Рабочего стола, Проводника, меню «Пуск» и им подобных. Также можно установить запрет на определеные горячие клавиши и всевозможные меню. Если интересуют только эти аспекты ограничений — ниже см. программу Deskman.

Ограничения функций Интернета представлены весьма поверхностно. Они заменяют один из компонентов Семейной безопасности: блокировка доступа к сайтам. Безусловно, любой файрволл по этой части будет оптимальным решением. Отсутствие же возможности хотя бы задать маску для веб-узлов делает данный раздел WinLock маловажным для опытного пользователя.

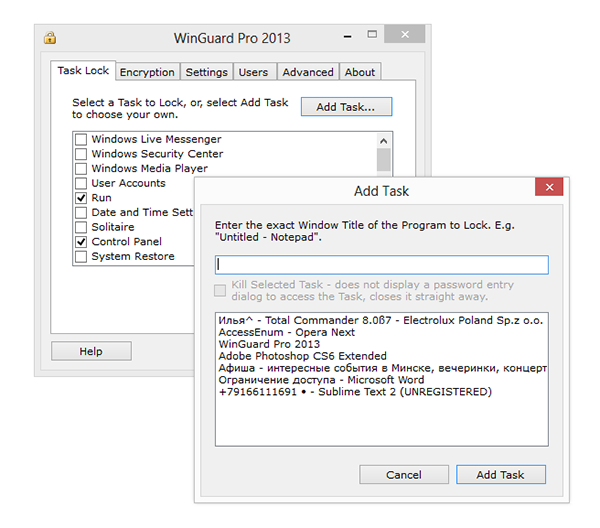
Кроме названных разделов, следует упомянуть «Доступ», где доступно управление приложенями. Любую программу легко занести в черный список по названию либо ручным добавлением.

В разделы «Файлы» и «Папки» можно поместить данные, которые необходимо скрыть от других пользователей. Пожалуй, не хватает парольной защиты доступа (для этого нужно обратиться к помощи других программ, см. ниже).

## WinGuard

Рисунок 3.

WinGuard

[](https://www.ixbt.com/soft/images/security-tweaks/3.png)

WinGuard можно использовать для блокировки приложений и разделов Windows, а также для шифрования данных. Программа распространяется в двух редакциях — бесплатной и Advanced. Функциональные отличия между ними невелики — несколько опций в одноименной вкладке «Advanced». Среди них отключение Internet Explorer, Проводника, процесса установки, записи файлов на USB.

Контроль над запуском приложений осуществляется во вкладке «Task Lock». Если нужной программы нет в списке, ее можно добавить самостоятельно, указав название в заголовке либо выбрав из списка открытых в данный момент приложений (аналогично WinLock). Если же сравнивать функцию блокировки с Security Administrator, в случае с WinGuard можно отключить ограничения для администраторского аккаунта. Однако настроить черный список приложений для каждого пользователя нельзя.

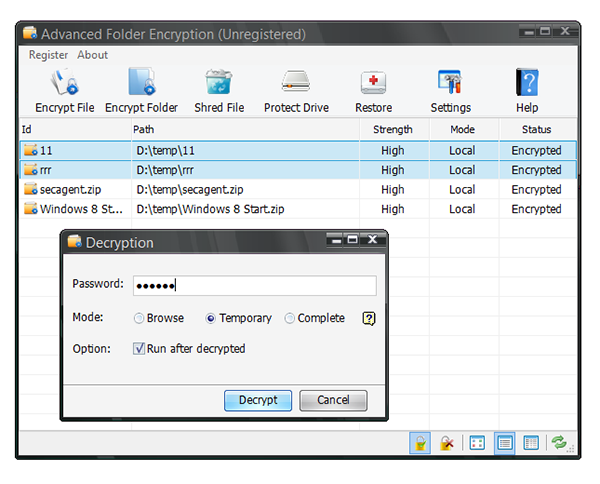
Шифрование доступно посредством раздела Encryption. Реализован пользовательский интерфейс неудобно: нельзя составить список для обработки, нет контекстного меню. Все, что нужно сделать — это указать директорию, которая будет являться и исходной, и конечной. Все содержащиеся файлы будут зашифрованы в 128-битный AES (Advanced Encryption Standard). Аналогичным образом производится расшифровка.

Таким образом, функциональность достаточно бедная, даже если взять во внимание платную версию.

## Advanced Folder Encryption

Рисунок 4.

Advanced Folder Encryption

[](https://www.ixbt.com/soft/images/security-tweaks/4.png)

Еще одна программа для AES-шифрования данных, и все же отличие от WinGuard весьма заметно.

Во-первых, выбор файлов для шифрования происходит быстрее. Не нужно выбирать каждую папку по-отдельности, достаточно составить список директорий и файлов. При добавлении Advanced Folder Encryption требует выставить пароль для шифрования.

Вы, в программе нет возможности указать метод защиты, вместо этого позволяется выбрать метод Norman, High или Highest.

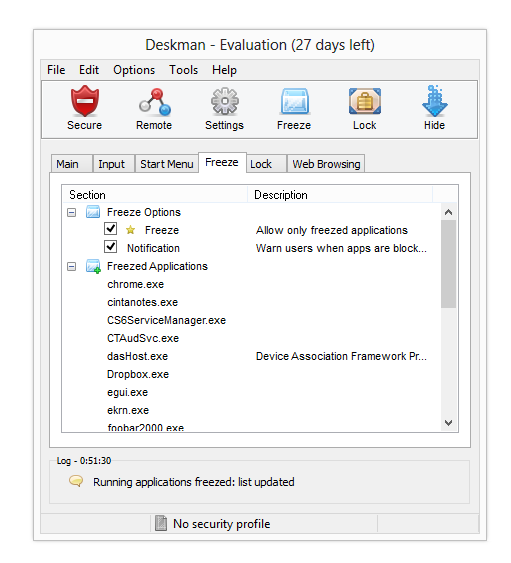
Второй удобный момент — шифрование через контекстное меню и расшифровка файлов одним кликом. Нужно понимать, что без установленной Advanced Folder Encryption данные не удастся просмотреть даже зная пароль. В этом отличие от архиваторов, которыми можно запаковать файлы в зашифрованный и всюду доступный exe-архив.

При выборе большого количества файлов для шифрования, как было замечено, не срабатывает кнопка отмены. Поэтому нужно быть осторожным, чтобы не получить результат в виде битого файла.

## Deskman

Рисунок 5.

Deskman



Программа для ограничения доступа к элементам интерфейса и системным разделам. Пожалуй, тут ее уместно сравнить с Security Administrator за той разницей, что Deskman более сконцентрирован на Рабочем столе. Системные опции также присутствуют, но это, скорее, то, что не подошло в другие разделы: отключение кнопок перезагрузки, Панели управления и другие смешанные опции.

В разделе Input — отключение горячих клавиш, функциональных кнопок и функций мыши. Помимо имеющегося списка, можно определить сочетания клавиш самостоятельно.

## Выводы

В результате проделанной работы мы убедились в том, что существует много различных программных средств для запрета доступа к файлам и папкам, но большинство их них платные, и предлагают излишне сложный интерфейс. Была изучена необходимая по теме литература и собрана информация для разработки собственного программного средства с учетом достоинств и недостатков, уже существующих на рынке.

# ГЛАВА 2 РАЗРАБОТКА ПРОГРАММНОГО СРЕДСТВА

**Задание:** Разработка программного средства запрещающего доступ к указанным папкам компьютера, запуск определенного списка файлов, запрещающего изменять системное время компьютера и устанавливающего указанные обои на рабочий стол.

## 2.1 Выбор программного обеспечения

В качестве операционной системы выберем ОС Windows 10.

К ее преимуществам относят:

* высокий запас по производительности;
* огромное количество программного обеспечения, доступного для скачивания;
* высокий уровень безопасности (относится как к защите от вредоносного ПО, так и от атак на виртуальные машины);
* возможность индивидуальной разработки ПО (обеспечивается поддержкой контейнеризации Kubernetes, широкими возможностями для масштабирования);
* работа с Windows Subsystem for Linux: позволяет разрабатывать ПО для операционной системы Linux, включая и виртуальные машины.

Клиентская операционная система осуществляет две основные функции: она предоставляет пользователю ряд тех или иных сервисов и управляет ресурсами компьютера, на котором она выполняется. Собственно, выбор операционной системы и определяется, во-первых, тем, какие у нее имеются ресурсы, а во-вторых, тем, какие сервисы требуются пользователю, — не все операционные системы способны работать с тем или иным аппаратным обеспечением, да и запросы пользователя (в том числе корпоративного) порой бывают столь высоки, что выбор операционных систем, способных их удовлетворить, оказывается весьма невелик.

Перечислим наиболее часто встречающиеся потребности пользователя:

Возможность применять офисные приложения (то есть готовить документы с помощью текстовых процессоров, электронных таблиц, средств презентационной графики и т.д.).

Возможность обращаться к ресурсам локальной сети и Интернета (например, к сетевым принтерам, файлам на сетевом диске или на Web-сайтах, к Web-приложениям и почтовым серверам).

Возможность пользоваться корпоративными приложениями, например входящими в состав системы управления предприятием. Последнее нередко косвенно влечет за собой такую потребность, как доступ к той или иной СУБД, — многие системы управления предприятиями используют архитектуру «клиент-сервер», требующую наличия на рабочем месте пользователя клиентской части СУБД, используемой в такой системе.

Надежность, средства защиты данных, устойчивость к сбоям.

## 2.2 Планирование информационной безопасности

Для обеспечения безопасной работы пользователя необходимо создать учетную запись входящую в группу Пользователи, но не входящую в группу Администраторы, либо создать учетную запись в другой группе с соответствующими ограничениями.

Ограничение доступа пользователей к файлам и папкам компьютера необходимо для обеспечения безопасности данных и сохранения конфиденциальности.

* Защита от несанкционированного доступа. Ограничение доступа к файлам и папкам компьютера позволяет предотвратить несанкционированный доступ к конфиденциальным данным, таким как финансовые документы, личные данные, бизнес-планы и т.д.
* Предотвращение случайного удаления или изменения данных. Ограничение доступа к файлам и папкам компьютера может предотвратить случайное удаление или изменение данных, которые могут быть важными для работы компании или организации.
* Управление правами доступа. Ограничение доступа к файлам и папкам компьютера позволяет управлять правами доступа для каждого пользователя, что обеспечивает более эффективное управление информацией.
* Сохранение конфиденциальности. Ограничение доступа к файлам и папкам компьютера помогает сохранить конфиденциальность данных, которые могут быть важными для компании или организации, так как доступ к ним могут иметь только уполномоченные пользователи.
* Защита от вирусов и вредоносных программ. Ограничение доступа к файлам и папкам компьютера может предотвратить заражение компьютера вирусами и вредоносными программами, которые могут нанести ущерб компании или организации.

Ограничение запуска определенных приложений пользователями может быть необходимо по нескольким причинам:

* Безопасность. Некоторые приложения могут быть опасными для компьютера и данных на нем. Ограничение запуска этих приложений может предотвратить возможные угрозы безопасности.
* Производительность. Некоторые приложения могут занимать большое количество ресурсов компьютера, что может снижать производительность системы. Ограничение запуска этих приложений может помочь улучшить производительность компьютера.
* Несанкционированное использование. Ограничение запуска некоторых приложений может предотвратить их использование без разрешения, что может привести к нарушению политики компании или организации.
* Сохранение конфиденциальности. Ограничение запуска некоторых приложений может помочь сохранить конфиденциальность данных, которые могут быть важными для компании или организации.
* Соответствие законодательству. В некоторых случаях компании или организации могут быть обязаны ограничивать запуск определенных приложений в соответствии с законодательством.

Запрещение пользователям изменять системное время может быть необходимо по нескольким причинам:

* Синхронизация с другими системами. Если компьютер подключен к сети, то его системное время должно быть синхронизировано с другими компьютерами и серверами в сети. Если пользователь изменит системное время, то это может нарушить синхронизацию и создать проблемы в работе сети.
* Учет времени работы. Некоторые программы и системы могут использовать системное время для учета времени работы. Если пользователь изменит системное время, то это может повлиять на точность учета времени работы и создать проблемы в отчетности.
* Защита от вредоносного ПО. Некоторые вредоносные программы могут изменять системное время для обхода защитных механизмов, например, для продления срока действия сертификатов безопасности. Запрещение пользователям изменять системное время может помочь предотвратить такие атаки.
* Сохранение целостности данных. Если пользователь изменит системное время, то это может повлиять на целостность данных, например, на даты создания и изменения файлов. Запрещение пользователям изменять системное время может помочь сохранить целостность данных и предотвратить ошибки в работе программ.
* Соответствие законодательству. В некоторых случаях компании или организации могут быть обязаны запрещать пользователям изменять системное время в соответствии с законодательством. Например, для соблюдения требований к учету рабочего времени или криптографической защите данных.

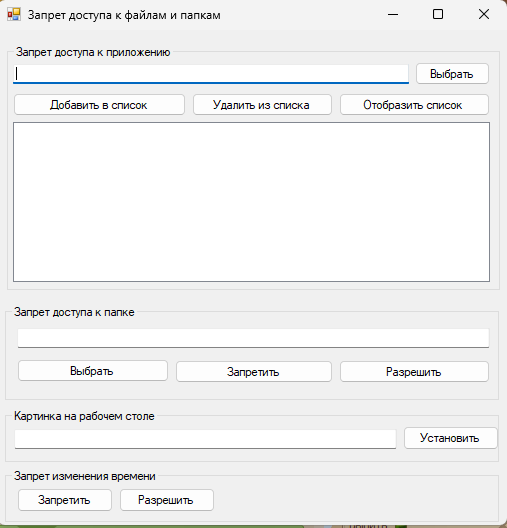
## 2.3 Разработка интерфейса программного средства

Создадим проект и разместим на главной форме приложения основные элементы управления с поясняющими надписями.

Внешний вид спроектированной формы представлен на рисунке 6.

Рисунок 6.

Внешний вид спроектированной формы.

****

Работа с реестром Windows заключается в создании и удалении веток и ключей реестра и присвоении им необходимых значений.

Для получения значений указанного ключа реестра используется следующая конструкция:

s = (string)Registry.GetValue ("HKEY\_CURRENT\_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer\\DisallowRun",”KEY”, "Empty");

Тут мы получаем значение ключа KEY и в случае его отсутствия возвращаем значение EMPTY

Для создания и присвоения значения ключу реестра используется следующая конструкция:

Registry.SetValue("HKEY\_CURRENT\_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer\\DisallowRun",”KEY”, "Empty");

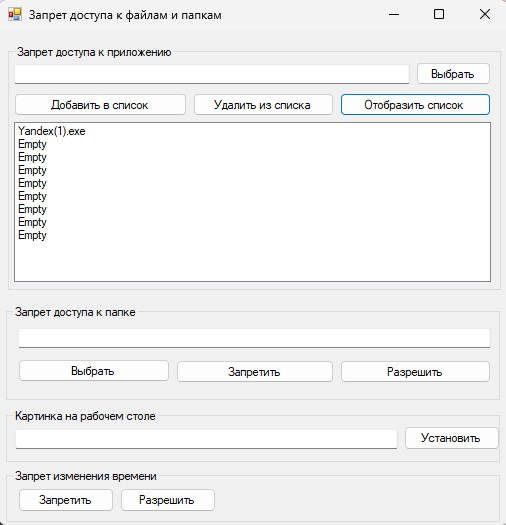
Тут значению ключа KEY присваивается строка “Empty”

Прочитав ветки реестра по пути HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\DisallowRun мы получим пронумерованный список приложений доступ к которым запрещен пользователю в системе. Каждый ключ представляет собой имя EXE файла. Видно, что такой запрет легко обойти если просто переименовать файл.

Приложение с выведенным списком программ, запрещенных к запуску представлено на рисунке 7.

Рисунок 7.

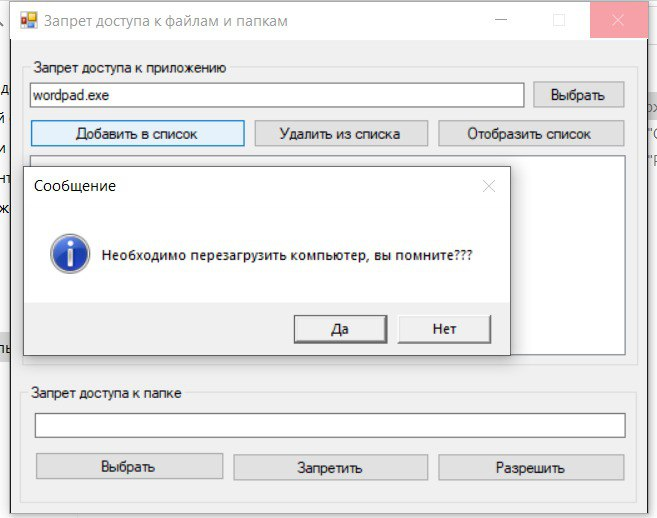
Список запрещенных для запуска программ в реестре.



Указав программу в списке и нажав кнопку «Удалить из списка» можно разрешить запуск ранее запрещенной программы. Нажатием кнопки «Выбрать» и указанием необходимого исполняемого файла с последующим добавлением его в список запрещенных программ можно запретить запуск определенных программ. После внесения изменений в список запрещенных программ программа напоминает о необходимости перезагрузки для вступления изменений в силу. Предупреждение о перезагрузке представлено на рисунке 8.

Рисунок 8.

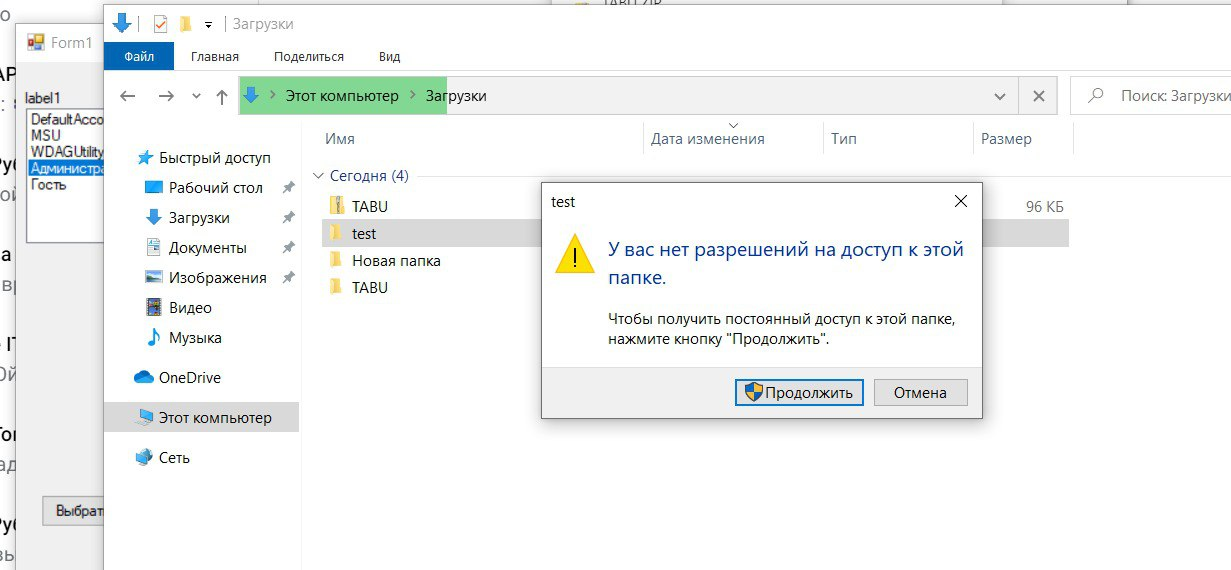
Предупреждение о перезагрузке.



После вступления изменений в силу при попытке запуска запрещенной программы операционная система выведет на экран предупреждающее сообщение, вид которого представлен на рисунке 9.

Рисунок 9.

Предупреждение о запрете запуска приложения.



Аналогичным образом осуществляется запрет и разрешение на доступ к указанной папке.

Программа так же позволяет осуществить смену рисунка рабочего стола, на рабочем столе можно разместить логотип компании, подсказки горячих клавиш или любую другую необходимую информацию.

Для запрета изменения времени пользователем системы созданы 2 кнопки в разделе запрета изменения времени. Запрет изменения времени автоматически подразумевает и запрет изменения системной даты.

В процессе проделанной работы было разработано программное средство, для запрета доступа к определенным файлам и папкам на диске компьютера для поддержания необходимого уровня безопасности системы.

# ЗАКЛЮЧЕНИЕ

В ходе выполнения курсовой работы была проведена аналитическая работа, по результатам которой было выявлено, что системный реестр Windows предоставляет средства для защиты доступа к файлам и папкам.

Были исследованы основные методы защиты данных, используемые в Windows, такие как User Account Control (UAC) и механизм управления доступом (Access Control Lists - ACLs).

В результате экспериментов было установлено, что методы аутентификации и авторизации, предоставленные Windows, обеспечивают надежную защиту данных. На основании результатов экспериментов было выявлено, что правильно настроенные ACLs и UAC могут быть использованы для предотвращения несанкционированного доступа к файлам и папкам.

Были проанализированы существующие методы защиты данных с помощью системного реестра, а именно атрибуты файлов и каталогов, политики безопасности Windows, управление правами доступа и другие.

Разработаны методы и алгоритмы защиты данных, позволяющие установить эффективную защиту файлов и папок.

Проведенные исследования показали, что использование системного реестра является эффективным инструментом для защиты данных на компьютере. Применение различных методов управления правами доступа и атрибутами файлов дает возможность обеспечить высокий уровень безопасности личных данных пользователей.

Таким образом, путем реализации разработанных методов и алгоритмов защиты данных, можно обеспечить эффективную защиту от несанкционированного доступа к файлам и папкам на компьютере.

Однако несмотря на то, что системный реестр Windows предоставляет средства для защиты файлов и папок, существуют уязвимости, которые могут быть использованы злоумышленниками для получения несанкционированного доступа к данным. Одной из таких уязвимостей является использование слабых паролей.

Для повышения уровня защиты данных необходимо следить за качеством паролей, использовать многофакторную аутентификацию и правильно настраивать системные средства защиты доступа к файлам и папкам.

Таким образом, использование системных средств защиты доступа к файлам и папкам через системный реестр Windows является эффективным методом защиты данных от несанкционированного доступа. Однако, для обеспечения надежной защиты необходимо правильно настроить ACLs и UAC, следить за качеством паролей и использовать многофакторную аутентификацию.

# СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

# Бэллью Дж., Дантеман Дж. Зачищаем Windows, или как значительно ускорить работу компьютера, очистив его от накопившегося хлама Издательство: Символ-Плюс 2008

# Колисниченко Д.Н. Секреты, настройка и оптимизация реестра Windows 7 Издательство: БХВ-Петербург 2010

# Кокорева О. Реестр Windows 7 Издательство: БХВ-Петербург Год: 2010

# Рэнд Моримото, Майкл Ноэл, Гай Ярдени, Омар Драуби, Эндрю Аббат, Крис Амарис Microsoft Windows Server 2012. Полное руководство Издательство: Вильямс 2013

# Уильям Р. Станек. Windows 7 для продвинутых // Издательство: Питер 2011

# Уильям Р. Станек Microsoft Windows 8. Справочник администратора Издательство: БХВ-Петербург 2014

# Уильям Р. Станек Windows 7. Справочник администратора Издательство: Русская Редакция, БХВ-Петербург 2010

# Уильям Р. Станек Windows Server 2008. Справочник администратора Издательство: БХВ-Петербург Год: 2008

# Чекмарев А.Н. Microsoft Windows Server 2008 (в подлиннике) Издательство: БХВ-Петербург 2008

# Чекмарев А. Н. Microsoft Windows 7. Руководство администратора Издательство: БХВ-Петербург Год: 2010

# Jordan Krause Windows Server 2012 R2 Administrator Cookbook Издательство: Packt Publishing 2015

# ПРИЛОЖЕНИЕ А

Текст программы.

using Microsoft.Win32;

using System;

using System.Collections.Generic;

using System.ComponentModel;

using System.Data;

using System.Drawing;

using System.IO;

using System.Linq;

using System.Security.AccessControl;

using System.Text;

using System.Threading.Tasks;

using System.Windows.Forms;

namespace ZAPRET

{

public partial class Form1 : Form

{

public Form1()

{

InitializeComponent();

}

private void button1\_Click(object sender, EventArgs e)

{

openFileDialog1.FileName = "Yandex.exe";

openFileDialog1.DefaultExt = ".exe";

openFileDialog1.Filter = "EXE files (.exe)|\*.exe";

if (openFileDialog1.ShowDialog() == DialogResult.Cancel)

return;

string filename = openFileDialog1.FileName;

textBox1.Text = Path.GetFileName(filename);

}

private void button4\_Click(object sender, EventArgs e)

{

string s;

listBox1.Items.Clear();

for (int i = 1; i < 10; i++)

{

s = (string)Registry.GetValue("HKEY\_CURRENT\_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer\\DisallowRun",

i.ToString(), "Empty");

listBox1.Items.Add(s + Environment.NewLine);

}

}

private void button3\_Click(object sender, EventArgs e)

{

int i;

string s;

i = listBox1.SelectedIndex + 1;

textBox1.Text = i.ToString();

Registry.SetValue("HKEY\_CURRENT\_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer\\DisallowRun", i.ToString(), "Empty");

listBox1.Items.Clear();

for (int j = 1; j < 10; j++)

{

s = (string)Registry.GetValue("HKEY\_CURRENT\_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer\\DisallowRun",

j.ToString(), "Empty");

listBox1.Items.Add(s + Environment.NewLine);

}

MessageBox.Show(

"Необходимо перезагрузить компьютер, вы помните???",

"Сообщение",

MessageBoxButtons.YesNo,

MessageBoxIcon.Information,

MessageBoxDefaultButton.Button1,

MessageBoxOptions.DefaultDesktopOnly);

}

private void button2\_Click(object sender, EventArgs e)

{

string s;

const string userRoot = "HKEY\_CURRENT\_USER";

const string subkey = "Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer";

const string keyName = userRoot + "\\" + subkey;

Registry.SetValue(keyName, "DisallowRun", listBox1.SelectedIndex + 1, RegistryValueKind.DWord);

Registry.SetValue(keyName + "\\" + "DisallowRun", "1", textBox1.Text);

listBox1.Items.Clear();

for (int i = 1; i < 10; i++)

{

s = (string)Registry.GetValue("HKEY\_CURRENT\_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer\\DisallowRun",

i.ToString(), "Empty");

listBox1.Items.Add(s + Environment.NewLine);

}

MessageBox.Show(

"Необходимо перезагрузить компьютер, вы помните???",

"Сообщение",

MessageBoxButtons.YesNo,

MessageBoxIcon.Information,

MessageBoxDefaultButton.Button1,

MessageBoxOptions.DefaultDesktopOnly);

}

private void button5\_Click(object sender, EventArgs e)

{

if (folderBrowserDialog1.ShowDialog() == DialogResult.OK)

{

textBox2.Text = folderBrowserDialog1.SelectedPath;

}

}

private void button6\_Click(object sender, EventArgs e)

{

try

{

string folderPath = textBox2.Text;

string adminUserName = Environment.UserName;// getting your adminUserName

DirectorySecurity ds = Directory.GetAccessControl(folderPath);

FileSystemAccessRule fsa = new FileSystemAccessRule(adminUserName, FileSystemRights.FullControl, AccessControlType.Deny);

ds.AddAccessRule(fsa);

Directory.SetAccessControl(folderPath, ds);

MessageBox.Show("Доступ к папке запрещен");

}

catch (Exception ex)

{

MessageBox.Show(ex.Message);

}

}

private void button7\_Click(object sender, EventArgs e)

{

try

{

string folderPath = textBox2.Text;

string adminUserName = Environment.UserName;// getting your adminUserName

DirectorySecurity ds = Directory.GetAccessControl(folderPath);

FileSystemAccessRule fsa = new FileSystemAccessRule(adminUserName, FileSystemRights.FullControl, AccessControlType.Deny);

ds.RemoveAccessRule(fsa);

Directory.SetAccessControl(folderPath, ds);

MessageBox.Show("Доступ к папке разрешен");

}

catch (Exception ex)

{

MessageBox.Show(ex.Message);

}

}

private void listBox1\_SelectedIndexChanged(object sender, EventArgs e)

{

}

private void button8\_Click(object sender, EventArgs e)

{

openFileDialog1.FileName = "Yandex.exe";

if (openFileDialog1.ShowDialog() == DialogResult.Cancel)

return;

string filename = openFileDialog1.FileName;

textBox3.Text = filename;

Registry.SetValue("HKEY\_CURRENT\_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System", "Wallpaper", textBox3.Text);

}

}

}