СОДЕРЖАНИЕ

[ВВЕДЕНИЕ 3](#_Toc136331447)

[1 ОПИСАНИЕ ПРЕДМЕТНОЙ ОБЛАСТИ 4](#_Toc136331448)

[2 РАЗРАБОТКА ПРОГРАММНОГО СРЕДСТВА 8](#_Toc136331449)

[РЕЗУЛЬТАТЫ И ИХ АНАЛИЗ 12](#_Toc136331450)

[ЗАКЛЮЧЕНИЕ 13](#_Toc136331451)

[Список использованных источников 14](#_Toc136331452)

[Приложение А 15](#_Toc136331453)

# 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 является 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.

# 1 ОПИСАНИЕ ПРЕДМЕТНОЙ ОБЛАСТИ

**Системный реестр Windows: что это такое и как он работает**

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.

# 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.

**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.

**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.

1. 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.

2. 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.

3. Управление правами доступа. Ограничение доступа к файлам и папкам компьютера позволяет управлять правами доступа для каждого пользователя, что обеспечивает более эффективное управление информацией.

4. 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.

5. 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:

1. Безопасность. Некоторые приложения могут быть опасными для компьютера и данных на нем. Ограничение запуска этих приложений может предотвратить возможные угрозы безопасности.

2. Производительность. Некоторые приложения могут занимать большое количество ресурсов компьютера, что может снижать производительность системы. Ограничение запуска этих приложений может помочь улучшить производительность компьютера.

3. Несанкционированное использование. Ограничение запуска некоторых приложений может предотвратить их использование без разрешения, что может привести к нарушению политики компании или организации.

4. Сохранение конфиденциальности. Ограничение запуска некоторых приложений может помочь сохранить конфиденциальность данных, которые могут быть важными для компании или организации.

5. 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:

1. 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.

2. 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.

3. 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.

4. 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.

5. 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.

**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 1.

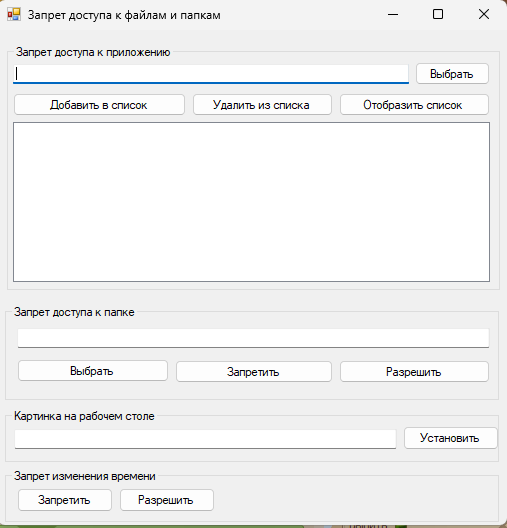
****

Рисунок 1. Внешний вид спроектированной формы.

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

Для работы с реестром на Delphi можно использовать стандартную библиотеку функций Windows API. Вот примеры некоторых операций с реестром:

1. Чтение значения из реестра:

var

Reg: TRegistry;

begin

Reg := TRegistry.Create;

try

Reg.RootKey := HKEY\_LOCAL\_MACHINE;

if Reg.OpenKey('Software\Microsoft\Windows\CurrentVersion', False) then

begin

ShowMessage(Reg.ReadString('ProgramFilesDir'));

Reg.CloseKey;

end;

finally

Reg.Free;

end;

end;

2. Запись значения в реестр:

```

var

Reg: TRegistry;

begin

Reg := TRegistry.Create;

try

Reg.RootKey := HKEY\_CURRENT\_USER;

if Reg.OpenKey('Software\MyApp', True) then

begin

Reg.WriteString('MySetting', 'MyValue');

Reg.CloseKey;

end;

finally

Reg.Free;

end;

end;

3. Удаление значения из реестра:

var

Reg: TRegistry;

begin

Reg := TRegistry.Create;

try

Reg.RootKey := HKEY\_CURRENT\_USER;

if Reg.OpenKey('Software\MyApp', True) then

begin

Reg.DeleteValue('MySetting');

Reg.CloseKey;

end;

finally

Reg.Free;

end;

end;

4. Удаление ключа из реестра:

var

Reg: TRegistry;

begin

Reg := TRegistry.Create;

try

Reg.RootKey := HKEY\_CURRENT\_USER;

if Reg.DeleteKey('Software\MyApp') then

ShowMessage('Key deleted')

else

ShowMessage('Key not found');

finally

Reg.Free;

end;

end;

Нужно обратить внимание, что для работы с реестром необходимы права администратора.

Для настройки протокола TCP/IP через реестр необходимо знать соответствующие ключи и значения в реестре Windows.

Например, для настройки IP-адреса и маски подсети можно использовать следующие ключи:

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\IPAddress

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\SubnetMask

Например, чтобы задать IP-адрес 192.168.0.1 и маску подсети 255.255.255.0, можно использовать следующий код:

var

Reg: TRegistry;

begin

Reg := TRegistry.Create;

try

Reg.RootKey := HKEY\_LOCAL\_MACHINE;

if Reg.OpenKey('SYSTEM\CurrentControlSet\Services\Tcpip\Parameters', True) then

begin

Reg.WriteString('IPAddress', '192.168.0.1');

Reg.WriteString('SubnetMask', '255.255.255.0');

Reg.CloseKey;

end;

finally

Reg.Free;

end;

end;

Для применения изменений необходимо перезагрузить сетевой адаптер или выполнить команду "ipconfig /renew" в командной строке.

Изменение имени компьютера и рабочей группы через реестр:

1. Откройте редактор реестра, нажав Win+R и введя команду regedit.

2. Перейдите к следующему разделу: HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName.

3. Внутри этого раздела найдите параметр ComputerName и дважды кликните на нем.

4. Измените значение параметра на новое имя компьютера и нажмите ОК.

5. Перейдите к разделу HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\ComputerName\ActiveComputerName.

6. Внутри этого раздела найдите параметр ComputerName и дважды кликните на нем.

7. Измените значение параметра на новое имя компьютера и нажмите ОК.

8. Перейдите к разделу HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters.

9. Внутри этого раздела найдите параметр Domain и дважды кликните на нем.

10. Измените значение параметра на новое имя рабочей группы и нажмите ОК.

Настройка параметров сетевой защиты через реестр:

1. Откройте редактор реестра, нажав Win+R и введя команду regedit.

2. Перейдите к следующему разделу: HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy.

3. Внутри этого раздела находятся различные подразделы, отвечающие за разные типы сетей и защиты.

4. Для изменения параметров защиты для конкретного типа сети выберите соответствующий подраздел.

5. Внутри подраздела находятся параметры, отвечающие за различные аспекты защиты, например, блокирование определенных портов или протоколов.

6. Дважды кликните на параметре, который вы хотите изменить, и измените его значение.

7. Нажмите ОК, чтобы сохранить изменения.

Изменение имени подключения через реестр:

1. Откройте редактор реестра, нажав Win+R и введя команду regedit.

2. Педрейдите к следующему разделу: HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles.

3. Внутри этого раздела находятся подразделы, соответствующие различным сетевым подключениям.

4. Для изменения имени подключения выберите соответствующий подраздел.

5. Внутри подраздела найдите параметр ProfileName и дважды кликните на нем.

6. Измените значение параметра на новое имя подключения и нажмите ОК.

Приложение с выведенным списком программ, запрещенных к запуску представлено на рисунке 2.

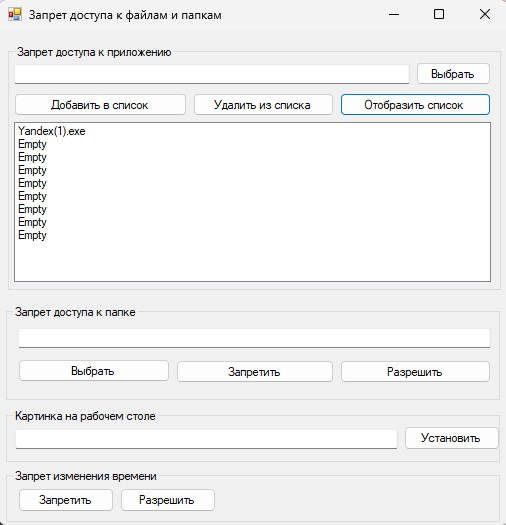


Рисунок 2. Список запрещенных для запуска программ в реестре.

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 рисунке3.

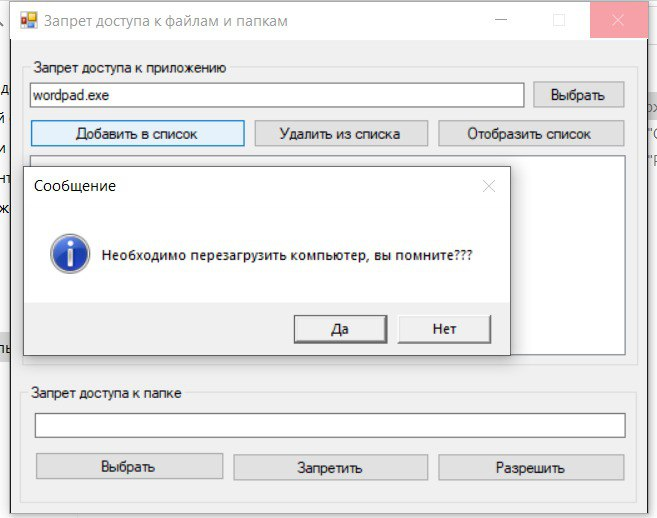


Рисунок 3. Предупреждение о перезагрузке.

После вступления изменений в силу при попытке запуска запрещенной программы операционная система выведет на экран предупреждающее сообщение вид которого представлен на рисунке 4.

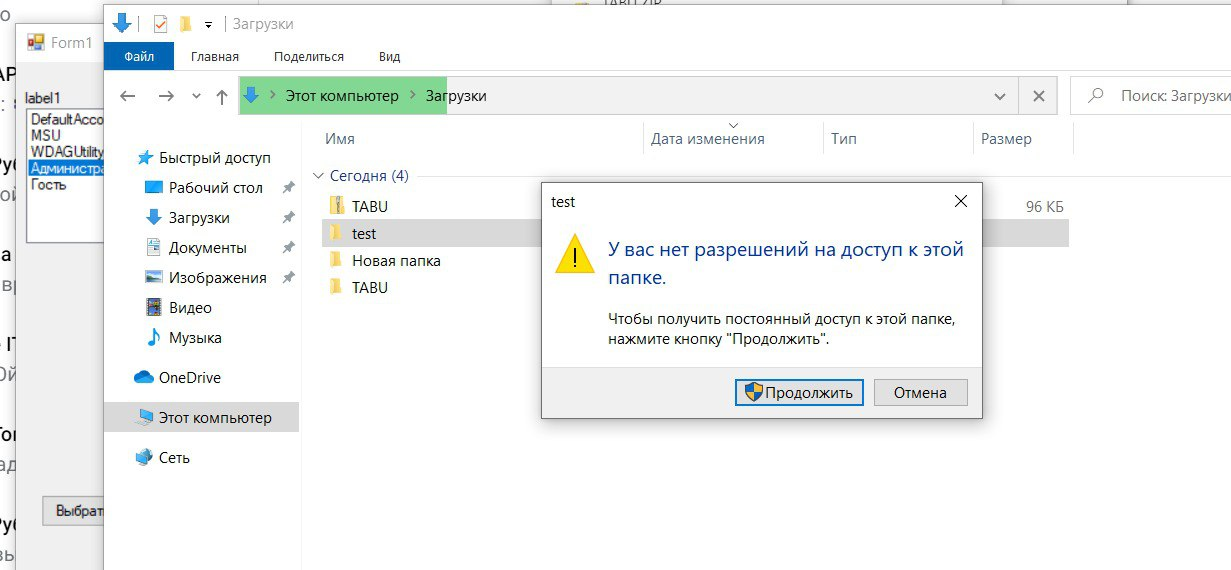


Рисунок 4. Предупреждение о запрете запуска приложения.

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.

# 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

# Приложение А

**Текст программы.**