Министерство транспорта Российской Федерации

Федеральное агентство железнодорожного транспорта

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«Дальневосточный государственный университет путей сообщения»

Кафедра: «Информационные технологии и системы»

К ЗАЩИТЕ ДОПУСТИТЬ

Заведующий кафедрой

\_\_\_\_\_\_\_\_\_\_\_\_ М.А. Попов

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_ 2019 г.

АВТОМАТИЗАЦИЯ УПРАВЛЕНИЯ ДОСТУПОМ В ИНФОРМАЦИОННОЙ СИСТЕМЕ

Пояснительная записка к магистерской диссертации

МД 10.04.01 ИБ2 ПЗ

Студент гр. ИБ2 М.Е. Иванов

Руководитель М.А. Попов

(доцент, к.т.н., доцент)

Нормоконтроль В.И. Шестухина

(доцент, к.п.н., доцент)

Хабаровск – 2019

Содержание

[Введение 3](#_Toc12834987)

[1 Постановка задачи исследования 5](#_Toc12834988)

[1.1 Описание исследуемого предприятия 5](#_Toc12834989)

[1.2 Решение проблемы использования дискреционного метода разграничения доступа 16](#_Toc12834990)

[2 Проектирование программного модуля для автоматизации разграничения доступа 24](#_Toc12834991)

[2.1 Диаграммы вариантов использования 24](#_Toc12834992)

[2.2 Диаграммы классов 30](#_Toc12834993)

[2.3 Диаграммы последовательности 35](#_Toc12834994)

[2.4 Диаграмма компонентов 42](#_Toc12834995)

[2.5 Диаграмма развертывания 43](#_Toc12834996)

[3 Выбор программных средств 46](#_Toc12834997)

[3.1 Язык программирования 46](#_Toc12834998)

[3.2 Среда разработки 46](#_Toc12834999)

[4 Руководство пользователя 48](#_Toc12835000)

[5 Руководство администратора 62](#_Toc12835001)

[Заключение 77](#_Toc12835002)

[Список используемых источников 78](#_Toc12835003)

[Основные определения 80](#_Toc12835004)

Введение

Информация всегда была важнейшей составляющей любой сферы деятельности и со временем ее важность и объем постоянно увеличивались. В настоящий момент объемы информации даже в небольших организациях достигли очень высоких показателей. В современном мире огромное внимание уделяют безопасности информации и проблемы защиты информации приобретают все большее значение. Связано это с тем, что потеря информации может привести к огромным убыткам предприятий.

Одной из основных мер защиты информации от несанкционированного доступа является разграничение доступа пользователей информационной системы.

При использовании различных способов и методов защиты от угроз информации, нельзя забывать об удобстве использования данных мер пользователями и администраторами безопасности. В данной работе, в качестве способа защиты от несанкционированного доступа будет использоваться дискреционный метод разграничения доступа.

Дискреционный метод разграничения доступа также называется избирательным, контролируемым управлением доступом, разграничительным управлением доступом. Он реализует управление доступом пользователей к информационной системе на основе списков управления доступом.

Для управления доступом к объектам информационной системы дискреционный метод использует идентификационную информацию пользователя и список доступа, который содержит пользователей и ассоциированные с ними типы доступа. Во время запроса доступа, система производит поиск пользователя в списке прав доступа объекта информационной системы. В случае если пользователь там присутствует и разрешённый тип доступа включает требуемый тип,  система разрешает доступ к объекту. В противном случае запрещает доступ.

Дискреционный метод разграничения доступа из-за своей гибкости, позволяет администратору безопасности произвести более тонкую настройку доступа к каждому объекту информационной системы. Несмотря на это, у этого метода существует значительный недостаток. Заключается он в том, что для настройки информационной системы администратору безопасности необходимо затратить огромное количество времени. Соответственно, контроль и поддержание этих настроек в актуальном состоянии также требуют больших временных затрат.

Существует закрытая и открытая системы дискреционного метода. Под закрытой системой понимается такая система, в которой изначально объект никому не доступен и в списке прав доступа описываются разрешения пользователей. Под открытой – та, в которой к объектам информационной системы все пользователи имеют полный доступ, а в списке доступа описывается список ограничений пользователей.

Целью данной магистерской диссертации является проектирование и разработка программного продукта, предназначенного для автоматизации управления доступом в информационной системе. Этот продукт позволит добиться сокращения временных затрат для настройки и поддержания системы в актуальном состоянии.

Магистерская диссертация состоит из трех основных глав, заключения и списка используемых источников.

В первой главе произведено исследование предметной области, выявлены основные проблемы использования дискреционного метода разграничения доступа и способы их решения.

Во второй главе описывается порядок разработки архитектуры предлагаемого программного обеспечения для дальнейшей ее реализации.

В третьей главе содержится руководство по использованию данного программного продукта.

1 Постановка задачи исследования

1.1 Описание исследуемого предприятия

В качестве исследуемого объекта было выбрано предприятие ООО «Продюсерский центр «Сделано в Хабаровске». Предприятие занимается созданием телевизионных программ о жизни Хабаровска и Хабаровского края, о истории Дальнего Востока во времена Великой Отечественной Войны и более ранние периоды.

Состав персонала организации:

* директор;
* администратор предприятия;
* бухгалтерия;
* монтажеры;
* операторы;
* сценаристы;
* звуковики.

Работники данной организации в процессе своей деятельности обрабатывают информацию, которая относится к двум видам защищаемой информации - это коммерческая тайне и персональные данные. Директор предприятия в силу занимаемой им должности имеет полный доступ к информации, которая хранится и обрабатывается на предприятии. Администратор соответственно отвечает за настройку информационной системы и поддержание ее в актуальном состоянии. Работники бухгалтерии в процессе работы обрабатывают персональные данные всех сотрудников и клиентов данной организации, а также они работают с информацией, которая считается коммерческой тайной.

Как было описано выше, деятельность данной организации напрямую связана с обработкой и хранением информации, которая относится к коммерческой тайне. Исходя из этого в процессе жизнедеятельности организации необходимо выполнять требования по защите информации, которые указаны в федеральном законе от 29.07.2004 N 98–ФЗ (ред. от 12.03.2014) "О коммерческой тайне". Данный Федеральный закон регулирует отношения, связанные с установлением, изменением и прекращением режима коммерческой тайны в отношении информации, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам. Режим коммерческой тайны считается установленным после принятия обладателем информации, составляющей коммерческую тайну, мер, указанных в части 1 статьи 10 «Охрана конфиденциальности информации». В части 1 этой статьи указано что меры по охране конфиденциальности информации, принимаемые ее обладателем, должны включать в себя:

* определение перечня информации, составляющей коммерческую тайну;
* ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;
* учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;
* регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско–правовых договоров.

Кроме информации, которая относится к коммерческой тайне, в информационной системе данного предприятия хранится и обрабатывается большой объем персональных данных клиентов и сотрудников. Отношения, которые связанны с обработкой персональных данных с использованием средств автоматизации регулируются Федеральным законом от 27.07.2006 N 152–ФЗ (ред. от 22.02.2017) "О персональных данных". Меры по обеспечению безопасности персональных данных при их обработке указаны в статье 19 данного закона. В данной статье представлены такие меры, как:

1. «оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных»;
2. обеспечение безопасности персональных данных достигается, в частности:
3. «определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных»;
4. «применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных»;
5. «применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации»;
6. «оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных»;
7. «учетом машинных носителей персональных данных»;
8. «обнаружением фактов несанкционированного доступа к персональным данным и принятием мер»;
9. «восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним»;
10. «установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных»;
11. «контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных».

Организационные и технические меры по обеспечению безопасности персональных данных, необходимых для выполнения требований к защите персональных данных, которые необходимо применять в соответствии с пунктом 2 статьи 19 Федерального закона № 152, указаны в приказе ФСТЭК России от 18.02.2013 N 21 (ред. от 23.03.2017) "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных". Требования к защите персональных данных содержатся в приказе ФСТЭК от 11 февраля 2013г №17 "Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах". Исходя из того, что состав мер защиты 17 и 21 приказа ФСТЭК совпадают, а в соответствии с 17 приказом, требования к защите персональных данных могут применятся для защиты персональных данных, содержащихся в негосударственных информационных системах, для рассмотрения необходимых мер, обратимся к 17 приказу ФСТЭК. В данном документе устанавливаются требования к обеспечению защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, от утечки по техническим каналам, несанкционированного доступа, специальных воздействий на такую информацию (носители информации) в целях ее добывания, уничтожения, искажения или блокирования доступа к ней при обработке указанной информации в государственных информационных системах. Также в документе не рассматриваются требования о защите информации, связанные с применением криптографических методов защиты информации и шифровальных (криптографических) средств защиты информации. Защита информации, содержащейся в государственной информационной системе, обеспечивается путем выполнения обладателем информации (заказчиком) и (или) оператором требований к организации защиты информации, содержащейся в информационной системе, и требований к мерам защиты информации, содержащейся в информационной системе.

Для данного приказа ФСТЭК существует методический документ «Меры защиты информации в государственных информационных системах». Этот методический документ детализирует организационные и технические меры защиты информации, принимаемые в государственных информационных системах в соответствии с Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденными приказом ФСТЭК России от 11 февраля 2013 г. № 17, а также определяет содержание мер защиты информации и правила их реализации. В методическом документе не рассматриваются содержание, правила выбора и реализации мер защиты информации, связанных с применением криптографических методов защиты информации и шифровальных (криптографических) средств защиты информации. Принятие таких мер защиты информации обеспечивается в соответствии с законодательством Российской Федерации.

Методический документ применяется для выбора и реализации в соответствии с пунктом 21 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11 февраля 2013 г. № 17, мер защиты информации в информационных системах, направленных на обеспечение:

* «конфиденциальности информации (исключение неправомерного доступа, копирования, предоставления или распространения информации) »;
* «целостности информации (исключение неправомерного уничтожения или модифицирования информации) »;
* «доступности информации (исключение неправомерного блокирования информации) ».

Реализация мер, представленных в данном методическом документе требует составления модели угроз информационной системы, создание, аттестацию и внедрение системы защиты и использование сертифицированных средств для обеспечения защиты информации в информационной системе предприятия. Для выполнения этих мер требуется длительный срок, поэтому было решено провести базовую реализацию некоторых мер уже имеющимися средствами, то есть внутренними средствами операционной системы Windows. Данные средства позволяют реализовать меры управления доступом субъектов доступа к объектам доступа 1 и 2.

Согласно пункту 3.2 Управление доступом субъектов доступа к объектам доступа (УПД), мера защиты УПД 1 «Управление (Заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей, необходимо предоставить пользователям права доступа к объектам доступа информационной системы, основываясь на задачах, решаемых пользователями в информационной системе». Предоставление прав доступа связано с реализацией методов управления доступом.

Требования к реализации методов разграничения доступа указаны в мере защиты УПД 2 «Реализация необходимых методов управления доступом (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа. В соответствии с этой мерой защиты, в информационной системе для управления доступом субъектов доступа к объектам доступа должны быть реализованы установленные оператором методы управления доступом, назначены типы доступа субъектов к объектам доступа и реализованы правила разграничения доступа субъектов доступа к объектам доступа».

Методы управления доступом должны реализовываться в зависимости от особенностей функционирования информационной системы предприятия, с учетом угроз безопасности информации и должны включать один или комбинацию следующих методов:

* дискреционный метод управления доступом, предусматривающий управление доступом пользователей информационной системы к объектам информационной системы на основе идентификационной информации пользователя и для каждого объекта доступа – списка, содержащего набор субъектов доступа (групп субъектов) и ассоциированных с ними типов доступа;
* ролевой метод управления доступом пользователей, который предусматривает управление доступом пользователей информационной системы к объектам информационной системы на основе совокупности действий и обязанностей, которые связанны с определенным видом деятельности пользователя;
* мандатный метод управления доступом, предусматривающий управление доступом пользователей информационной системы к объектам информационной системы на основе сопоставления классификационных меток каждого пользователя информационной системы и каждого объекта информационной системы, отражающих классификационные уровни пользователя информационной системы и объектов информационной системы, являющиеся комбинациями иерархических и неиерархических категорий.

Типы доступа при их реализации должны включать в себя операции по чтению, записи, удалению, выполнению и иные операции, которые разрешены к выполнению пользователем или запускаемому от его имени процессу при доступе к объектам доступа информационной системы.

Правила разграничения доступа реализуются на основе установленных оператором списков доступа или матриц доступа и должны обеспечивать управление доступом пользователей (групп пользователей) и запускаемых от их имени процессов при входе в систему, доступе к техническим средствам, устройствам, объектам файловой системы, запускаемым и исполняемым модулям, объектам систем управления базами данных, объектам, создаваемым прикладным и специальным программным обеспечением, параметрам настройки средств защиты информации, информации о конфигурации системы защиты информации и иной информации о функционировании системы защиты информации, а также иным объектам доступа.

Правила разграничения доступа должны регламентироваться в организационно – распорядительных документах оператора по защите информации.

Дискреционный метод управления доступом реализуется при любом развертывании системы защиты, так как является основным методом, доступным в операционной системе. Он обладает большим функционалом и является встроенным механизмом операционной системы, используемой на предприятии. Однако, дискреционный метод не лишен проблем при его реализации в информационной системе. Одним из его недостатков является чрезмерная сложность корректной настройки и поддержания существующих настроек в процессе эксплуатации информационной системы предприятия. Кроме того, дискреционный метод разграничения доступа позволяет организовывать движение информации в информационных потоках предприятия. Разделение информационных потоков предприятия может осуществляется с использованием различных методов и технологий, при этом обмен информацией между пользователями при отсутствии функциональной системы электронного документооборота, как правило, осуществляется с использованием общих папок или сетевых дисковых хранилищ, доступ к которым открыт у какой–то группы пользователей или у всех пользователей.

Мандатный доступ и дискреционный доступ действуют независимо друг от друга. То есть, если, например, присвоить папке метку конфиденциальности "строго конфиденциально" и одновременно разрешить пользователю работу с этой папкой средствами дискреционного доступа, то пользователь сможет работать с ней, только если он имеет уровень конфиденциальности не меньше чем "строго конфиденциально". И наоборот, если папке с меткой конфиденциальности "конфиденциально" запретить доступ пользователю средствами дискреционного доступа, этот пользователь не сможет работать с ней, даже если и имеет уровень конфиденциальности не меньше "конфиденциально". В связи с этим возможно появление двух видов ошибок при настройке методов разграничения доступа:

* отсутствие доступа к информации;
* наличие неправомерного доступа к информации.

Настройка дискреционного метода включает в себя определение типов доступа, используемых при разграничении доступа. Типы доступа включают в себя стандартные и специальные разрешения NTFS для файлов и папок.

К стандартным разрешениям для папок относятся:

* чтение (Read);
* запись (Write);
* список содержимого папки (List folder contents);
* чтение и выполнение (Read&Execute);
* изменение (Modify);
* полный доступ (Full control);
* особые разрешения (Special Permission).

К стандартным разрешениям для файлов относятся:

* чтение (Read);
* запись (Write);
* чтение и выполнение (Read&Execute);
* изменение (Modify);
* полный доступ (Full control);
* особые разрешения (Special Permission).

К специальным разрешениям для файлов и папок относятся:

* обзор папок / Выполнение файлов;
* содержание папки / Чтение данных;
* чтение атрибутов;
* чтение дополнительных атрибутов;
* создание файлов / Запись данных;
* создание папок / Дозапись данных;
* запись атрибутов;
* запись дополнительных атрибутов;
* удаление;
* удаление подпапок и файлов;
* чтение разрешений;
* смена разрешений;
* смена владельца.

Чем более широкий набор типов доступа используется на предприятии, тем большая сложность настройки дискреционного метода, а следовательно усложняется процедура проверки правильности настройки разграничения доступа. Возникает необходимость использования программного средства, направленного на упрощение контроля правильности настройки дискреционного доступа.

Исходя из описанного, для защиты информации на предприятии должны применятся сертифицированные средства защиты информации. Все работники предприятия в той или иной степени участвуют как в обработке персональных данных, таких как видео или аудио информация, так и в обработке коммерческой информации, так как данная информация представляет большую ценность для организации.

Организационные и технические меры для обеспечения безопасности ПДн, необходимые для соответствия требованиям указаны в приказе ФСТЭК России от 18.02.2013 N 21 (ред. от 23.03.2017) "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных". Для данного приказа имеется методический документ «Меры защиты информации в государственных информационных системах». Этот документ более подробно раскрывает меры защиты, применяемые в соответствии с требованиями к защите информации, не составляющей государственную тайну. Также в нем определены правила реализации мер защиты информации.

В методическом документе не рассматриваются вопросы связанные с применением криптографических методов и средств защиты информации. В данном методическом документе будет рассматриваться раздел связанный с управлением доступом в информационной системе. Согласно требованиям, для управления доступом необходимо использовать один или несколько методов разграничения доступа, таких как дискреционный, мандатный или ролевой методы. Так как мандатный метод разграничения доступа применяется в основном в секретном делопроизводстве, то в данной работе он рассматриваться не будет.

Исходя из рассуждений о том, что большие организации не испытывают проблем использования дорогостоящих средств защиты информации, реализующих и мандатный и роевой методы разграничения доступа, и имеют большой штат сотрудников, данная работа направлена на создания средства управления доступом для небольших организаций, содержащих небольшой штат сотрудников. В случае малого количества персонала ролевой метод разграничения доступа будет проблематичным решением, так как в процессе исполнения трудовых обязанностей у пользователя может кардинально изменятся его трудовая обязанность. Это влечет за собой необходимость либо постоянно редактировать имеющиеся роли, которые в определенный момент могут оказаться избыточными, либо создавать дополнительные роли, в случае которых также возрастает нагрузка на администратора из-за необходимости не только настроить роли, но и удалять за ненадобностью.

Исходя из описанного выше, в данной работе предлагается использовать дискреционный метод разграничения доступа. Данный выбор обусловлен тем, что это мощный и гибкий инструмент, который позволяет настраивать доступ пользователей для любых целей. Также плюсом дискреционного метода разграничения доступа является возможность его реализации встроенными средствами операционной системы. Однако, у данного метода существует очень серьезный недостаток, который не позволяет его использовать в полной мере. Этот недостаток связан с очень большими затратами рабочего времени администратора системы. Администратору необходимо для каждого пользователя настраивать права доступа к каждому объекту информационной системы, так как возможных прав доступа около десятка, то настройка дискреционного доступа для организации состоящей даже из десяти человек требует несколько дней непрерывной работы. В случае, если необходимо редактировать права доступа пользователям, администратор опять вынужден тратить огромное количество сил и времени. Именно решение данного недостатка дискреционного доступа предложено в данной работе.

1.2 Решение проблемы использования дискреционного метода разграничения доступа

Основные цели построения любой системы защиты информации – обеспечение [конфиденциальности](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BD%D1%84%D0%B8%D0%B4%D0%B5%D0%BD%D1%86%D0%B8%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D1%81%D1%82%D1%8C), [целостност](https://ru.wikipedia.org/wiki/%D0%A6%D0%B5%D0%BB%D0%BE%D1%81%D1%82%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8)и и [доступност](https://ru.wikipedia.org/wiki/%D0%94%D0%BE%D1%81%D1%82%D1%83%D0%BF%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8)и защищаемых информационных ресурсов. При этом обеспечение информационной безопасности (ИБ) – это комплексная задача, решаемая параллельно по целому ряду направлений: правовому, организационному и техническому.

Для реализации аспектов ИБ можно использовать различные методы разграничения доступа. Метод доступа к объекту – операция, которая определена для данного объекта. Ограничить доступ к объекту возможно именно с помощью ограничения возможных методов доступа.

Рассмотрим достоинства и недостатки дискреционного и мандатного методов разграничения доступа.

«Разграничение доступа — совокупность правил, регламентирующих порядок и условия доступа субъекта к [объектам информационной системы](http://www.dataved.ru/2014/02/controlled-access-concepts.html). В качестве объекта рассматривают информацию и информационные ресурсы, носители информации, процессы обработки информации. Правила называют правами доступа или политиками безопасности.»

Дискреционный контроль доступа позволяет субъектам определять права доступа к объектам при условии наличия прав собственности на данные объекты. Данный подход обеспечивает гибкость и динамичность в изменении полномочий субъекта. При всей наглядности и гибкости возможных настроек разграничительной политики доступа к ресурсам, данной модели присущи серьезные недостатки. Основной из них – это излишне детализированный уровень описания отношений субъектов и объектов, что приводит к усложнению процедуры администрирования системы защиты. Причем это происходит как при задании настроек, так и при поддержании их в актуальном состоянии при включении в схему разграничения доступа новых субъектов и объектов. Как следствие, усложнение администрирования может приводить к возникновению ошибок, росту количества уязвимостей и увеличению возможностей доступа к информации со стороны внешних и внутренних нарушителей. «Существенным недостатком дискреционных моделей является то, что в ходе функционирования структура информационных систем изменяется таким образом, что субъекты и объекты могут меняться местами. Так, информационные системы рассматривались ранее как объект управления, в то время как человек-пользователь являлся субъектом управления. Но при включении человека в информационную систему его роли разделились на исполнительную и управляющую. Человек-исполнитель теперь является объектом управления, а человек с ролью управления является субъектом управления.»

«С целью устранения недостатков матричных моделей были разработаны так называемые многоуровневые модели защиты, классическими примерами которых являются модель конечных состояний Белла и Ла-Падулы, а также решетчатая модель Д. Деннинг. Многоуровневые модели предполагают формализацию процедуры назначения прав доступа посредством использования так называемых меток конфиденциальности или мандатов, назначаемых субъектам и объектам доступа.» Метки доступа субъекта определяются в соответствии с уровнем допуска лица к информации, а для объекта доступа – признаками конфиденциальности информации. Все возможные уровни допуска четко определены и упорядочены по возрастанию секретности. «В матричной модели действуют два основных правила:

1. Пользователь может читать только объекты с уровнем допуска не выше его собственного.

2. Пользователь может изменять только те объекты, уровень допуска которых не ниже его собственного.

Таким образом, многоуровневая модель предупреждает возможность преднамеренного или случайного снижения уровня конфиденциальности защищаемой информации за счет ее утечки. То есть эта модель препятствует переходу информации из объектов с высоким уровнем конфиденциальности и узким набором категорий доступа в объекты с меньшим уровнем конфиденциальности и более широким набором категорий доступа».

«Практика показывает, что многоуровневые модели защиты находятся гораздо ближе к потребностям реальной жизни, нежели матричные модели, и представляют собой хорошую основу для построения автоматизированных систем разграничения доступа.» Причем, так как отдельно взятые категории одного уровня равнозначны, то, чтобы их разграничить наряду с многоуровневой (мандатной) моделью, требуется применение матричной модели. На основе многоуровневых моделей возможно существенное упрощение задачи администрирования. Данный факт касается как исходной настройки разграничительной политики доступа (не требуется столь высокого уровня детализации задания отношения субъект-объект), так и последующего включения в схему администрирования новых объектов и субъектов доступа. «Мандатные модели применяются в случаях, если имеет место четкая централизованная система управления доступа, при которой каждый пользователь имеет ровно столько информации, сколько ему требуется, и безопасность или надежность данных является основным приоритетом. Обычно это большие системы, где функции всех членов строго регламентированы.» Однако информационная система является сложной динамической средой, что говорит о том, что информация в ней не привязана к уровням секретности так строго, как этого требуют мандатные модели разграничения доступа. Согласно выше сказанному, существенным недостатком, затрудняющим использование данной модели, является отсутствие гибкости, связанной с выделением и изменением полномочий. Можно сделать вывод, что классические модели не отвечают всем потребностям разграничения доступа в динамически изменяющейся среде информационных систем. Представленный недостаток можно разбить на две части.

Первая часть – это каким образом обеспечивается разграничение доступа к документам, которые находятся в стадии разработки. Ведь до присвоения метки конфиденциальности, документ необходимо подготовить и утвердить, только после этого ему присваивается метка и документ приобретает особый статус.

Вторая часть проблемы – это разграничение доступа к документам, не попадающим в уровни конфиденциальности. Ведь помимо документов, содержащих конфиденциальную информацию, документооборот предприятия содержит и ежедневно создаваемые объекты, которые также имеют ценность и значимость, а значит их тоже необходимо защищать.

Для соответствия требованиям по защите информации, при работе с секретным делопроизводством обязательно применение мандатного метода разграничения доступа. В виду простоты настройки и реализации, мандатный доступ лишь дополняется дискреционным, для разграничения доступа в горизонтали. В участках информационной системы, где отсутствует секретное делопроизводство, зачастую вообще не используют каких либо мер защиты, в лучшем случае при создании информационной системы, так как поддержание ее в актуальном состоянии требует больших временных затрат.

Практическая реализация будет заключаться в решении недостатка, представленного выше, с помощью реализации программного продукта. Программный продукт позволит производить настройку дискреционного доступа в простом для администратора виде и с минимальными временными затратами.

В тоже время, с целью обеспечения единых подходов к обеспечению разграничения доступа, непрерывного мониторинга и контроля состояния системы защиты, сокращения сроков модернизации, модификации и восстановления существующей системы разграничения доступа в ходе жизнедеятельности организации, значительную роль играет корректное отражение реализованной системы разграничения доступа в комплекте организационно-распорядительных документов.

Существующие механизмы дискреционного, мандатного, ролевого разграничения доступа позволяют обеспечить реализацию необходимых мер защиты информации, но само корректное и подробное описание применяемых политик настройки средств защиты и программных продуктов ведет к неоправданному росту объема разрабатываемых документов. Представьте объем матрицы доступа, в которой будет подробно расписано дискреционный принцип доступа даже для 30-50 пользователей, работающих в сети предприятия. Описание модели мандатного разграничения доступа как правило сводится к документированию высшего грифа конфиденциальности документов и весьма формальному описанию местоположения защищаемых ресурсов. Аналогичная проблема существует и при описании других моделей. Анализ вышеизложенного материала позволяет сделать вывод, что даже применение различных средств автоматизации процесса формирования и описания полномасштабной матрицы доступа принесут определенный положительный эффект, но это только половинчатая мера. Необходимо кардинальное решение данной проблемы. Одним из способов является переход от статической к динамической матрице доступа, формируемой на основе пула разрешенных маршрутов с обязательным автоматическим журналированием действий пользователя.

Для решения задачи по определению правил разграничения доступа к вновь создаваемым информационным ресурсам предлагается представить информационную систему в виде логически связанных узлов. Узел – это пользователь без привязки роли администратора или роли пользователя. Ввиду большого количества вариантов движения информационного ресурса в процессе его создания, корректировки (отладки), ознакомления, визирования, принятия решения и тому подобное, и сложности их описания (вариантов), предлагается непосредственное определение перечня допущенных узлов возложить на главенствующий сетевой узел на каждом этапе решения той или иной задачи.

Например, исполнитель на своем узле И1 после создания документа определяет порядок и права доступа к нему последующего узла работы с документом (начальник Н1). На данном этапе главенствующим узлом является И1. Начальник Н1 после выполнения своих функций ознакомления, визирования и т.п., определяет следующий узел и его права по отношению к документу. Доступ предыдущего узла И1 при этом может быть аннулирован. Основная идеология данного базируется на том постулате, что должностное лицо (главенствующий узел) в данный момент времени несет основную ответственность за содержание и обеспечение безопасности информационного ресурса.

При этом, выбор исполнителем И1 следующего узла, например Н1, осуществляется из набора разрешенных к взаимодействию узлов И1 – И3, Н1 – Н2 и т.д.

Использование данного подхода позволяет вместо описания всевозможных вариантов движения документа в матрице доступа описать только разрешенный набор взаимодействующих узлов, а документирование процесса ознакомления, модификации, удаления, передачи возлагается на автоматизированную систему журналирования действий каждого участника процесса.

Проведенный анализ показывает, что мандатный доступ дополняется дискреционным. Следовательно, расширение используемого функционала дискреционного метода разграничения доступа позволит улучшить гибкость в секретном делопроизводстве до момента получения документом метки конфиденциальности, а также позволит регулировать несекретные потоки информации в информационной системе.

Для решения описанного недостатка использования дискреционного метода разграничения доступа было принято решение о создании программного средства. Необходимо сразу уточнить, что данное программное средство не является средством защиты информации. Разработка приложения производилась в процессе прохождения производственной практики и для использования на конкретном предприятии.

В процессе проектирования программного продукта были выделены следующие функции:

* создание пользователем заявки на предоставление доступа;
* применение необходимых прав доступа администратором.

Создание пользователем заявки на предоставление доступа – пользователю необходимо заполнить форму с указанием требуемых прав доступа и соответствующего информационного ресурса. После заполнения пользователю необходимо подтвердить создание заявки. Созданная заявка отправляется в базу данных и не подлежит редактированию. Так же в базе данных содержится информация о создателе заявки. Созданная заявка отображается у пользователя на главной форме для отслеживания процесса обработки. Если администратор применит данную заявку, она будет отображаться на вкладке выполненные заявки со статусом выполнено. В случае отказа заявка также отображается на вкладке выполненные, но имеет статус отказ.

Применение необходимых прав доступа администратором – после создания заявки пользователем, администратор на главной форме увидит данную заявку. Также на главной форме отображаются данные пользователя, который создал эту заявку. Администратор может открыть заявку для просмотра, любые изменения в ней заблокированы. Если администратор принимает решение дать пользователю права, то необходимо нажать на кнопку применить, в противном случае отказать. В случае отказа заявка принимает статус отказ. В случае применения заявки отрабатывает вторая часть программного модуля. Данный модуль считывает необходимые права доступа, ресурсы информационной системы и имя пользователя, которому необходимо предоставить права. Программа применяет права доступа в автоматическом режиме. После обработки заявки она принимает статус выполнено.

Предлагаемое программное решение использует средства операционной системы Windows и служит инструментом для упрощения работы администратора в процессе настройки информационной системы и в процессе ее эксплуатации. Для проектирования данного программного средства был выбран объектно-ориентированный подход так как продукт с разбивается на модули для лучшего понимания структуры программы.

Для описания моделей, содержащихся в программном продукте, используется язык моделирования UML (Unified Modeling Language), считающийся стандартным средством при выборе ООП.

# 2 Проектирование программного модуля для автоматизации разграничения доступа

## 2.1 Диаграммы вариантов использования

Процесс проектирования любой системы необходимо начинать с определения задач, которые необходимо реализовать в процессе создания программного продукта. Для наглядного отображения задач используются диаграммы вариантов использования.

Суть данной диаграммы состоит в следующем: проектируемая система представляется в виде множества актеров, взаимодействующих с системой с помощью так называемых вариантов использования. При этом актером называется любой объект, субъект или система, взаимодействующая с моделируемой системой извне. В свою очередь вариант использования – это спецификация сервисов (функций), которые система предоставляет актеру. При этом в модели никак не отражается то, каким образом будет реализован этот набор действий.

Функционал работы модуля для создания заявок был подробно описан в первом разделе. Исходя из данного описания можно выделить актера, взаимодействующего с программой. В качестве актера может выступать администратор, пользователь и пользователь с расширенными правами. Общей задачей для всех типов пользователей является создание заявки на предоставление доступа в информационной системе. Помимо процесса создания заявки, пользователь с расширенными правами имеет функционал для согласования заявок, созданных обычными пользователями. Пользователь с расширенными правами подразумевается как начальник отдела, а пользователи - это работники его отдела. Начальник отдела имеет права согласовывать только заявки созданные внутри своего отдела. Администратор имеет право создавать заявки для всех работников организации, а также для их согласования. Но главным инструментом администратора является возможность применять заявку на предоставление доступа к информационной системе. Разработанная диаграмма вариантов использования функционала администратора представлена на рисунке 2.1.

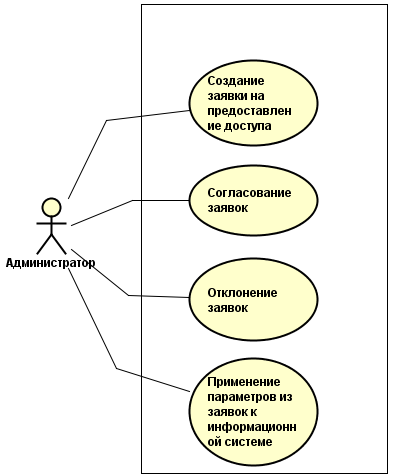


Рисунок 2.1 − Контекстная диаграмма вариантов использования функционала администратора

Исходя из описанного функционала можно выделить следующие варианты использования:

* создание заявки на предоставление доступа;
* согласование заявки;
* отклонение заявки;
* применение параметров из заявок к информационной системе.

Создание заявки на предоставление доступа – это вариант использования, при котором администратор создает для пользователя информационной системы заявку, в которой указываются права доступа к необходимым информационным ресурсам. На рисунке 2.2 изображена диаграмма, иллюстрирующая данный процесс.

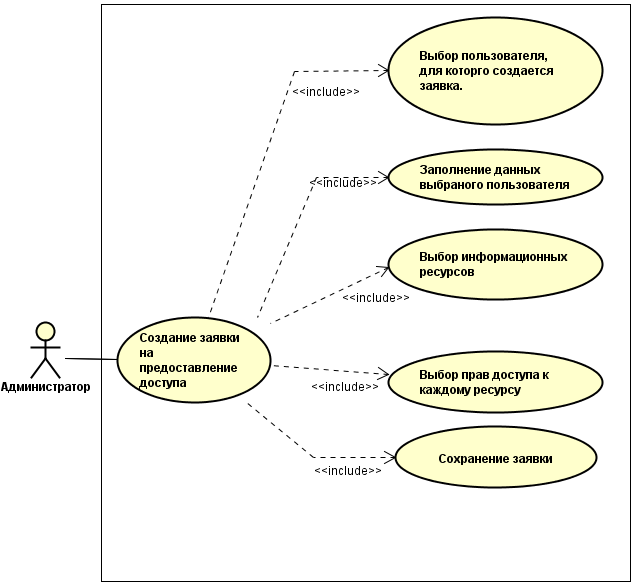


Рисунок 2.2 − Диаграмма вариантов использования «Создание заявки на предоставление доступа»

Согласование заявки – это процесс, при котором администратор открывает созданную заявку для просмотра и просматривает к каким ресурсам и какие права запрашиваются для пользователя. Если администратор согласен с данными, которые указаны в заявке, он ставит отметку о согласовании. В заявку вносятся данные о том, кто проводил процесс согласования, такие как фамилия, имя, отчество, должность и дата согласования. После внесения данных заявка сохраняется. На рисунке 2.3 изображена диаграмма, на которой показан данный вариант использования.

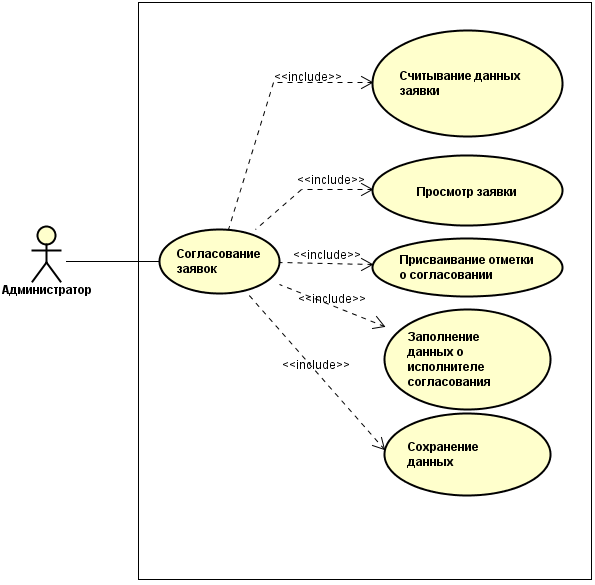


Рисунок 2.3 − Диаграмма вариантов использования «Согласование заявки»

В том случае, когда администратор не согласен с предоставляемыми правами к информационным ресурсам, он может отклонить заявку. Процесс отклонения заявки администратором возможен как на этапе согласования, так и после согласования, если согласование производил другой пользователь. Аналогично процессу согласования, в случае отклонения заявки вносятся данные о том, кто проводил процесс согласования, такие как фамилия, имя, отчество, должность и дата отклонения. Соответствующая диаграмма вариантов использования изображена на рисунке 2.4.

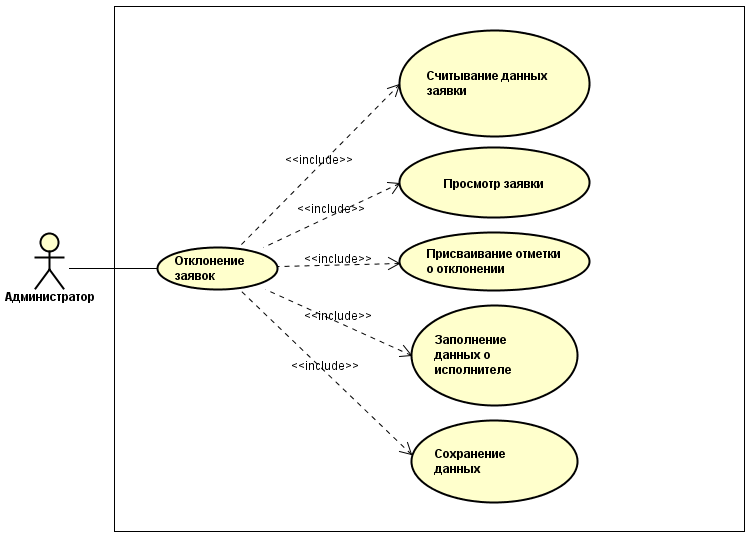


Рисунок 2.4 − Диаграмма вариантов использования «Отклонение заявки»

Последний вариант использования применение параметров из заявок к информационной системе необходим для внесения изменений в настройки системы согласно заявке. В данном случае администратору необходимо открыть заявку для просмотра и применить данные в заявке настройки. Применение настроек происходит автоматически за счет функционала программного продукта. При применении заявки, программный модуль считывает сохраненные в заявке данные о пользователе и находит соответствующего пользователя в информационной системе. Следующим шагом является считывание списка информационных ресурсов и соответствующие им права доступа. После выполнения данных действий, программный модуль изменяет настройки доступа для данного пользователя к каждому информационному ресурсу из заявки, предварительно удалив предыдущие права доступа. После изменения настроек доступа вносит данные о исполнителе, такие как фамилия, имя, отчество, должность и дата исполнения. Также заявке присваивается статус выполнено. Соответствующая диаграмма изображена на рисунке 2.5.

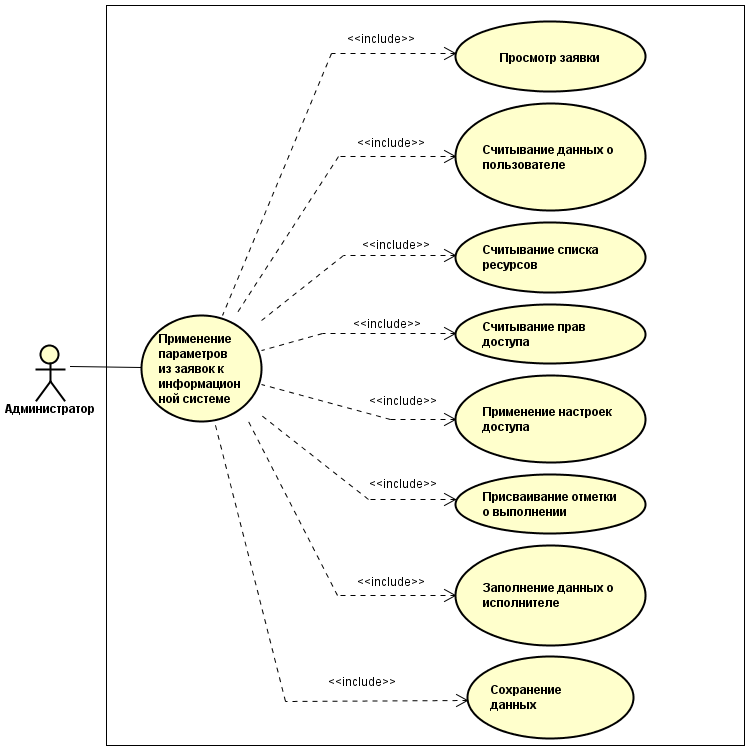


Рисунок 2.5 − Диаграмма вариантов использования «Применение параметров из заявки к информационной системе»

## 2.2 Диаграммы классов

Основой ООП при проектировании программного продукта являются классы и объекты. Класс представляет из себя абстрактный тип данных, который описывает какую-то часть предметной области. В свою очередь объект представляет собой его конкретный экземпляр. Диаграмма классов анализа является укрупненной абстракцией, отображающей общую структуру классов разрабатываемого приложения и взаимоотношений между ними. Класс анализа является более абстрактной сущностью, нежели класс, описанный некоторым фрагментом системы. Таким образом, класс анализа – это укрупненная абстракция, которая на концептуальном уровне (без точного определения атрибутов и операций) описывает некоторый фрагмент системы. Главное отличие в том, что они не содержат определений атрибутов и методов.

Назначение классов анализа:

* граничный класс – используется для моделирования взаимодействия между системой и актерами (пользователями, внешними системами или устройствами). Взаимодействие часто включает в себя получение или передачу информации, запросы на предоставление услуг и т. д. Граничные классы являются абстракциями диалоговых окон, форм, панелей, коммуникационных интерфейсов, интерфейсов периферийных устройств, интерфейсов API (англ. application program interface – интерфейс прикладных программ) и т. д. Каждый граничный класс должен быть связан как минимум с одним актером;
* управляющий класс – отвечает за координацию, взаимодействие и управление другими объектами, выполняет сложные вычисления, управляет безопасностью, транзакциями и т. п.
* класс сущности – используется для моделирования долгоживущей, нередко сохраняемой информации. Классы сущности являются абстракциями основных понятий предметной области – людей, объектов, документов и т. д., как правило, хранимых в табличном или ином виде.

На рисунке 2.6 показана диаграмма классов анализа для разрабатываемого приложения. На нем изображена связь между графическими составляющими программного модуля и определенными внутри сущностями. Главная форма данного приложения содержит актуальные и выполненные заявки разграничения доступа. Для создания новой заявки или просмотра созданной существует форма "Заявка". На данной форме для добавления пользователя необходимо вызвать форму "Пользователи", которая содержит диалоговое окно для выбора и добавления пользователя. Пользователь является сущностью класса "Субъект". Также на данной форме присутствует диалоговое окно для добавления ресурсов в список ресурсов для настройки прав доступа пользователей к этим ресурсам. Информационный ресурс является сущностью класса "Объект". Форма "Права доступа" также вызывается с формы для создания заявок. На данной форме пользователь при создании заявки указывает необходимые права доступа к каждому выбранному информационному ресурсу в системе. Диалоговое окно отвечает за процесс создания заявки на предоставление доступа. Заявка формируется из сущностей классов "Субъект", "Объект" и "Право доступа". Граничные классы интерфейса программного средства необходимы для визуального отображения процессов работы и отвечают за взаимодействие программного модуля с администратором информационной системы. Классы-сущности необходимы для создания различных экземпляров в процессе работы программы. Например, сущностями являются пользователи, ресурсы информационной системы и устройства.

Для того, чтобы получить в процессе проектирования углубленное представление структуры модуля, необходимо использовать диаграмму классов, которая наглядно отображает конечную структуру классов проектируемого программного модуля. Состав диаграммы классов аналогичен составу [диаграммы классов анализа](https://www.sites.google.com/site/anisimovkhv/learning/pris/lecture/tema13/tema13_2). В то же время классы анализа должны пройти процедуру строгой экспертизы на предмет их возможной декомпозиции на более мелкие и специализированные классы. При построении диаграммы окончательно должны быть определены атрибуты и операции классов.

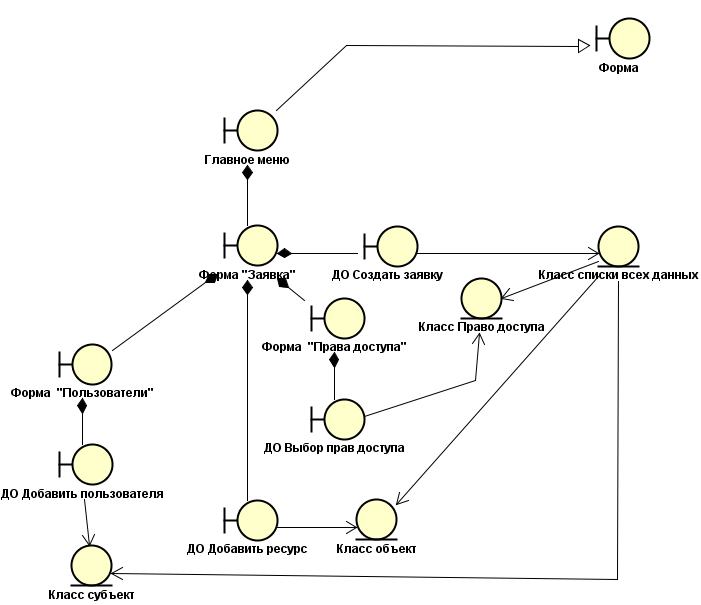


Рисунок 2.6 − Диаграмма классов анализа программного модуля для создания заявок разграничения доступа

Разрабатываемое приложение состоит из интерфейсов и методов для взаимодействия пользователя с приложением, а также для обработки данных. Для наглядного отображения структуры программного модуля на рисунке 2.7 представлена диаграмма классов.

На представленной диаграмме изображены классы. Содержимое классов представлено полями, конструкторами и методами.

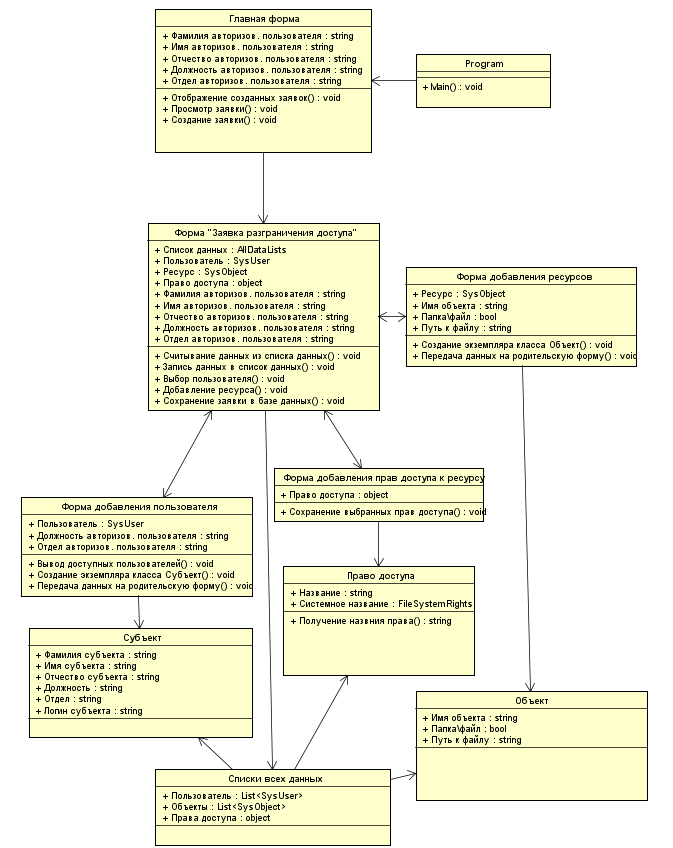


Рисунок 2.7 − Диаграмма классов программного модуля

Представленный на диаграмме класс Program является главной точкой входа в приложение, таким образом вся работа модуля начинается с данного класса. Он отвечает за процесс создания и отображения главной формы приложения.

Главный класс Главная форма, представленный на диаграмме, является главной формой программы, которую видит пользователь запуская программу. На данной форме отображаются созданные заявки. Класс имеет функционал для просмотра содержимого заявки, а также имеется метод, который позволяет создать новую заявку.

Форма "Заявка разграничения доступа" отвечает за отображение подробной информации о заявке в процессе просмотра или создания ее экземпляра. Все операции проводимые над заявкой совершаются пользователем на этой форме. На форме отображаются данные о пользователе, которому предоставляется доступ, список ресурсов, к которым предоставляют доступ и соответствующие права для каждого ресурса. При просмотре заявки на данной форме администраторы могут согласовывать и применять заявки.

Форма добавления пользователя отвечает за отображение возможных пользователей, для которых актер может создать заявку разграничения доступа. При выборе пользователя создает экземпляр класса "Субъект" и передает данные на форму заявок.

Форма добавления ресурсов представляет из себя диалоговое окно для выбора файлов или папок информационной системы, для которых настраивается доступ пользователя. При выборе ресурса создает объект класса "Объект" и передает данные на форму заявок в список ресурсов.

Форма добавления прав доступа вызывается с формы заявок для выбора пользователем прав, которые необходимо предоставить. После выбора прав доступа к ресурсу и их сохранения, для каждого права создается экземпляр класса "Право доступа", все экземпляры помещаются в массив прав и передаются на форму заявок.

Класс "Субъект" содержит в себе поля необходимые для хранения данных о пользователе информационной системы, для которого создается заявка на предоставление прав доступа.

Класс "Объект" предназначен для преобразования выбранного информационного ресурса в экземпляр класса. Это позволяет привести информацию о ресурсе к одному виду и упрощает хранение и использование данной информации.

Класс "Право доступа" содержит в себе два поля, предназначенные для хранения данных о конкретном праве доступа. В одном поле хранится название права на русском языке для удобства пользованием. Второе поле является полем типа FileSystemRights, и представляет из себя системный тип данных, предназначенный для работы с правами доступа. Хранит в себе название права доступа, представленное в операционной системе.

Также на данной диаграмме представлен класс AllDataLists. Данный класс представляет из себя список и предназначен для хранения всех существующих экземпляров классов, которые описаны выше. Экземпляр данного класса содержит всю информацию, необходимую для создания и исполнения заявки на предоставление доступа.

2.3 Диаграммы последовательности

Диаграммы последовательности необходимы для отображения структуры между объектами создаваемого приложения и взаимодействующего с ним актера, которые определенны при проектировании. Диаграмма последовательности наглядно отображает временной аспект взаимодействия. Она имеет два измерения. Одно измерение (слева-направо) указывает на порядок вовлечения экземпляров сущностей во взаимодействие. Крайним слева на диаграмме отображается экземпляр актера или объект, который является инициатором взаимодействия. Правее отображается другой экземпляр сущности, который непосредственно взаимодействует с первым и т.д. Второе измерение (сверху-вниз) указывает на порядок обмена сообщениями. Начальному моменту времени соответствует самая верхняя часть диаграммы. Масштаб на оси времени не указывается, поскольку диаграмма отображает лишь временную упорядоченность взаимодействия типа «раньше-позже». Также, данные диаграммы позволяют наглядно отобразить взаимодействие между данными элементами во времени и наглядно показать время жизни элементов. Процесс взаимодействия между актером и объектами разрабатываемого приложения происходит при помощи передачи сообщения. Передача сообщений происходит во время активности имеющихся объектов. Данная активность отображается на диаграмме при помощи прямоугольников, которые в свою очередь отображаются на линии жизни объекта. Помимо этого, на диаграммах последовательности присутствуют элементы, которые называются фрагменты. Фрагменты необходимы для отображения таких особенностей взаимодействия как циклы, условные операторы и т.д.

Для данного проектируемого программного модуля представлены четыре диаграммы последовательности, которые отображают подробную реализацию взаимодействия администратора с типовыми функциями программы. Подробное рассмотрение данных диаграмм позволяет лучше понять работу данных функций приложения.

Диаграмма, изображенная на рисунке 2.8, подробно описывает взаимодействие всех элементов программного модуля, которые необходимы для создания заявки разграничения доступа.

Для создания новой заявки разграничения доступа, администратор должен выбрать пункт Создать заявку. После выбора пункта откроется пустая форма Заявка разграничения доступа на которой администратору необходимо заполнить данные. В первую очередь необходимо заполнить данные пользователя, для которого создается заявка. Для этого администратор должен вызвать форму Пользователи. На открывшейся форме отображаются отделы и их работники, для которых возможно создать заявку разграничения доступа. После выбора пользователя форма закрывается, а данные переносятся на форму заявки. Следующим шагом необходимо добавить информационные ресурсы к которым необходимо предоставить доступ. Выбор ресурса происходит в диалоговом окне, в котором отображаются все ресурсы данного устройства. После выбора ресурса, окно закрывается, а данные о выбранном ресурсе добавляются в список ресурсов на форме заявки. Далее администратор должен

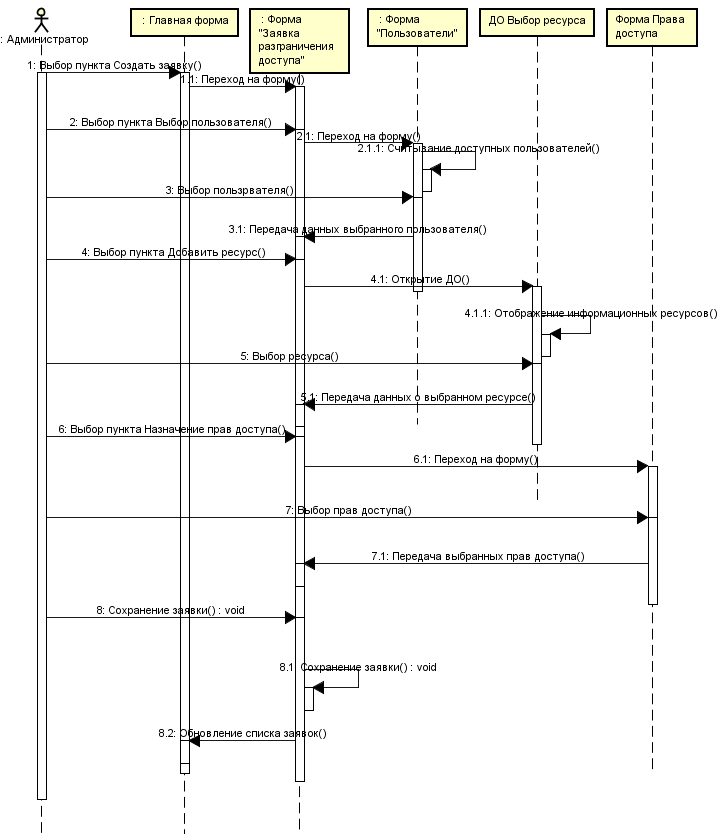


Рисунок 2.8 − Диаграмма последовательности создания администратором заявки разграничения доступа

для каждого выбранного ресурса указать права доступа пользователя. Для этого он выбирает информационный ресурс из созданного списка на форме заявки. При выборе ресурса из списка откроется форма прав доступа, на которой администратор может произвести выбор прав доступа. После выбора прав доступа происходит их передача на форму заявки. После настройки доступа ко всем ресурсам из списка администратору необходимо сохранить заявку. При сохранении заявки форма закрывается, а заявка отображается на главной форме.

Диаграмма, изображенная на рисунке 2.9, наглядно представляет процесс по согласованию заявки.

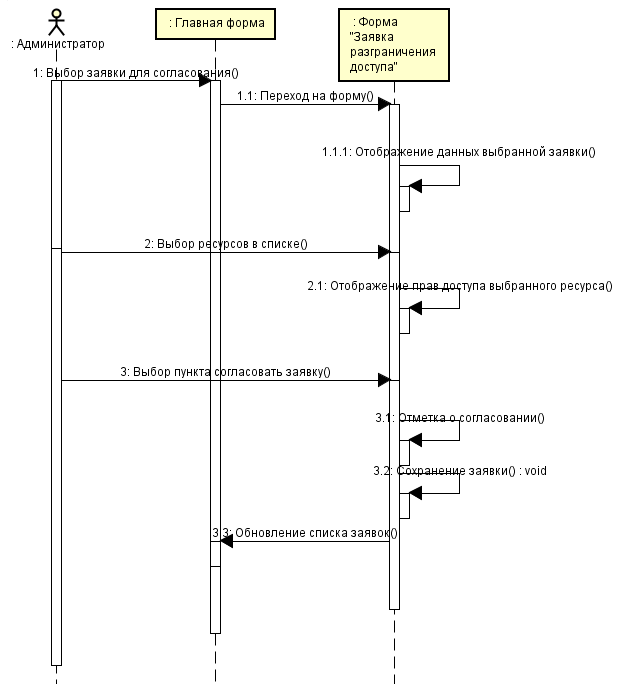


Рисунок 2.9 − Диаграмма последовательности согласования администратором заявки разграничения доступа

Для использования данной функции администратору необходимо на главной форме выбрать заявку на распределение доступа. После выбора заявки открывается форма "Заявка разграничения доступа" и на ней отображаются данные выбранной заявки. Администратор может путем выбора ресурсов на форме просмотреть права доступа которые необходимо предоставить. Для согласования заявки необходимо выбрать пункт Согласовать заявку. При согласовании заявки ей присваивается метка о согласовании и записываются данные о пользователе, который согласовал заявку, такие как фамилия, имя, отчество и должность, также сохраняется дата согласования. После внесения данных заявка сохранятся, форма заявки закрывается и происходит обновление списка заявок на главной форме.

Диаграмма, изображенная на рисунке 2.10, наглядно представляет процесс по отклонению заявки разграничения доступа.

Для использования данной функции администратору необходимо на главной форме выбрать заявку на распределение доступа. После выбора заявки открывается форма "Заявка разграничения доступа" и на ней отображаются данные выбранной заявки. Администратор может путем выбора ресурсов на форме просмотреть права доступа которые необходимо предоставить. В случае если администратор не согласен с запрашиваемыми правами он может отклонить данную заявку. Процедура отклонения доступна для созданных заявок и для согласованных заявок. Для отклонения заявки администратору необходимо выбрать пункт Отклонить заявку. При отклонении заявки ей присваивается метка о отклонении и записываются данные о пользователе, который отклонил заявку, такие как фамилия, имя, отчество и должность, также сохраняется дата отклонения. После внесения данных заявка сохранятся, форма заявки закрывается и происходит обновление списка заявок на главной форме.

Функция применения параметров к информационной системе необходима для того, чтобы пользователь, для которого была создана заявка, получил необходимые ему права доступа. Для использования этой функции администратору необходимо открыть заявку на главной форме. В открывшейся

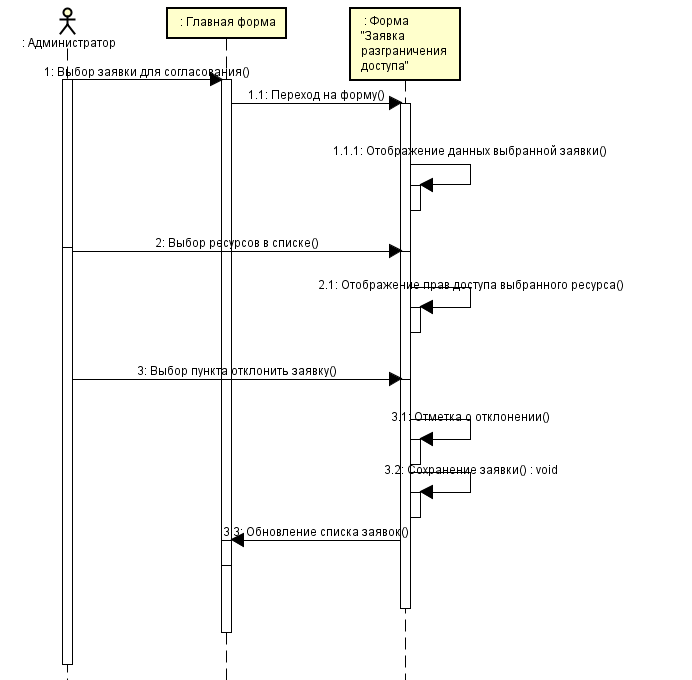


Рисунок 2.10 − Диаграмма последовательности отклонения администратором заявки разграничения доступа

форме он может просмотреть настраиваемые права доступа путем выбора информационных ресурсов из списка на форме. Для применения параметров администратору необходимо выбрать пункт Применить. Применение настроек к информационной системе происходит в автоматическом режиме. После применения параметров в заявку сохраняется метка о применении и данные о пользователе, который применил заявку, такие как фамилия, имя, отчество и должность. После происходит сохранение заявки, форма закрывается и на главной форме обновляется список заявок. Диаграмма, которая описывает данный процесс, представлена на рисунке 2.11.

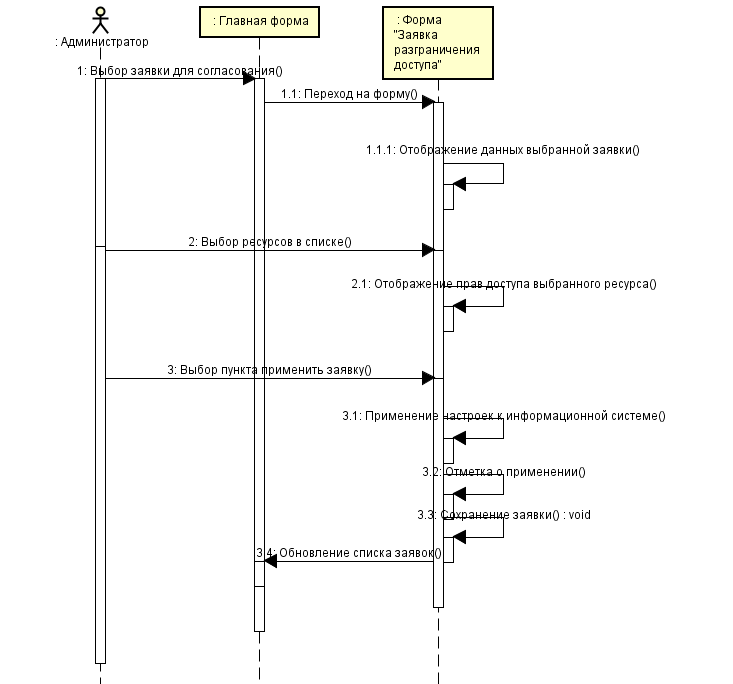


Рисунок 2.11 − Диаграмма последовательности изменения администратором настроек программного модуля

## 2.4 Диаграмма компонентов

Диаграмма компонентов представляет статическую структурную диаграмму, необходимую для определения разбиения программного продукта на составные компоненты и связи между ними. В качестве составных физических компонентов могут выступать файлы, библиотеки, исполняемые файлы, модули, пакеты и т.п.

При разработке диаграмм компонентов преследуются следующие цели:

* спецификация общей структуры исходного кода системы;
* спецификация исполнимого варианта системы.

Данная диаграмма обеспечивает согласованный переход от логического к физическому представлению системы в виде программных компонентов. Одни компоненты могут существовать только на этапе компиляции программного кода, другие – на этапе его исполнения. Разработанная при проектировании программного модуля для автоматизации разграничения доступа диаграмма компонентов представлена на рисунке 2.12.

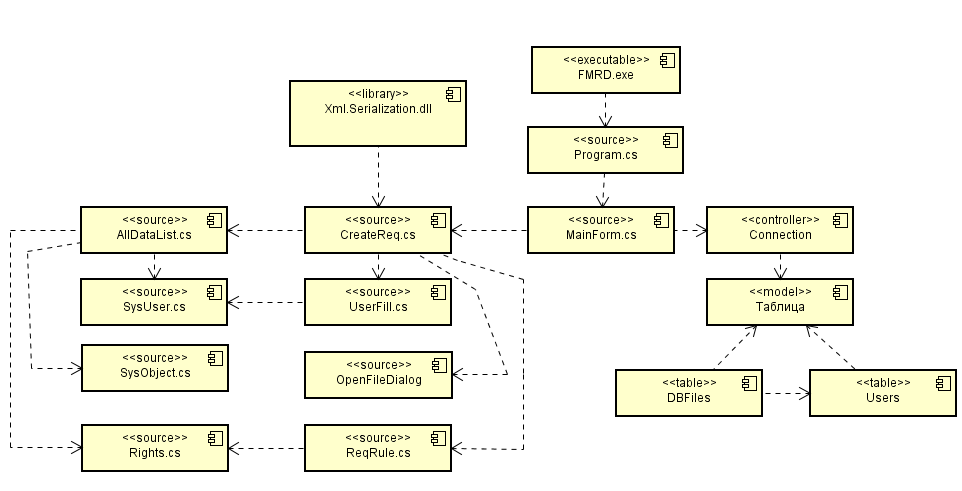


Рисунок 2.12 − Диаграмма компонентов программного модуля автоматизации разграничения доступа

## 2.5 Диаграмма развертывания

Для полного понимания физического представления об информационной системе необходима информация о топологии информационной системы и необходимых для функционирования программного средства аппаратных средствах. Кроме базовых сведений о устройствах, которые обрабатывают информацию, также в процессе проектирования необходимо определить то, как будет осуществляться связь между компонентами информационной системы и существует ли необходимость в использовании дополнительных ресурсов. При разработке однопользовательской локальной системы полностью отсутствует необходимость в разработке подобной диаграммы. Однако при разработке сетевых корпоративных приложений ситуация представляется совсем по-другому.

Во-первых, сложные информационные системы могут реализовываться на различных вычислительных платформах и технологиях доступа к базам данных. Наличие корпоративной сети требует решения целого комплекса дополнительных задач по рациональному размещению компонентов по узлам сети, что определяет общую производительность информационной системы.

Во-вторых, интеграция информационной системы с Интернетом определяет необходимость решения дополнительных вопросов при проектировании системы, таких как обеспечение безопасности и доступности информации для корпоративных клиентов.

Наконец, доступ и манипулирование данными в рамках двух- или трехуровневой технологии «клиент-сервер» также требуют размещения больших БД в различных сегментах корпоративной сети, их резервного копирования, архивирования, кэширования для обеспечения необходимой производительности системы в целом. Эти аспекты также требуют визуального представления с целью спецификации программных и технологических особенностей реализации распределенных архитектур.

Второй формой физического представления программной системы является диаграмма развертывания (размещения). Она применяется для представления общей конфигурации и топологии распределенной информационной системы, содержит сведения о распределении компонентов по отдельным узлам системы и каналом связи между аппаратными средствами (соединения).

Таким образом, диаграмма развертывания предназначена для визуализации элементов и компонентов системы, существующих лишь на этапе ее исполнения (runtime), к которым относятся исполнимые файлы, динамические библиотеки, таблицы БД и т. д. Те компоненты, которые не используются на этапе исполнения (например, исходные тексты программ), на диаграмме не показываются.

Основные цели, преследуемые при разработке диаграммы развертывания:

* распределение компонентов системы по ее физическим узлам;
* отображение физических связей между узлами системы на этапе исполнения;
* выявление узких мест системы и реконфигурация ее топологии для достижения требуемой производительности.

Элементами диаграммы развертывания являются узлы, компоненты и связи между ними.

Узел (англ. node) представляет собой некоторый физически существующий элемент системы. В качестве узла могут рассматриваться компьютеры, датчики, принтеры, модемы, цифровые камеры, сканеры и т.д. Графически узел изображается в форме трехмерного куба, внутри которого указывается его имя и, возможно, дополнительная информация в виде помеченного значения.

В качестве канала связи (соединения – англ. connection) между узлами выступает физическое соединение (например, оптоволоконная линия или спутниковая связь), ссылка на сайт в Интернет и т. д. Соединения показываются в виде ассоциации и изображаются линиями без стрелок. Наличие такой линии указывает на необходимость организации канала для обмена информацией между соответствующими узлами. Характер соединения может быть дополнительно специфицирован примечанием, помеченным значением или ограничением. На рисунке 2.13 представлена диаграмма размещения для разрабатываемого программного продукта. Серверная часть представляет из себя MS SQL Server 2012, на котором развернута база данных Enterprise. Клиентская часть разворачивается на компьютерах сотрудников. Для запуска не требует установки, но для работы программы необходимо наличие Framework 4.5.

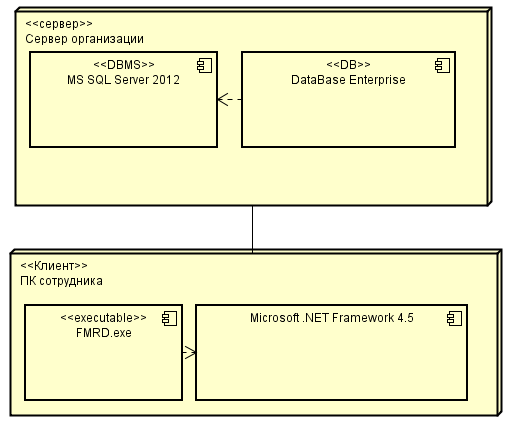


Рисунок 2.13 − Диаграмма развертывания программного модуля автоматизации разграничения доступа

# 3 Выбор программных средств

## 3.1 Язык программирования

В процессе проектирования данного приложения было решено использовать язык программирования C#. Этот язык программирования является объектно - ориентированным и относится к семье языков с C - подобным синтаксисом. На выбор данного языка повлияло наличие большого опыта разработки приложений на данном языке в процессе обучения, а так же то, что данный язык отличается простотой и функциональностью.

Несомненным плюсом данного языка является то, что он относится к классу объектно - ориентированных языков программирования. Объектно - ориентированный принцип программирования является самым распространённым принципом программирования на сегодняшний день. Данный принцип подразумевает представление программы в виде совокупности объектов, представленных экземплярами классов. Такое представление помогает более четко разделить данные приложения и программный код, а так же позволяет увеличить коэффициент повторного использования кода.

## 3.2 Среда разработки

В качестве среды разработки было выбрано программное решение от компании Microsoft под названием VisualStudio 2015 Community Edition. Данная среда разработки является бесплатной, полнофункциональной и расширяемой интегрированной средой разработки для создания современных приложений. Данная среда является весьма удобной для разработок, так как ее разработчики с каждым выпуском стараются учесть все пожелания пользователей данного продукта.

Данный продукт был выбран по нескольким причинам:

поддержка языка программирования C#;

− удобство интерфейса;

− наличие возможностей навигации по коду, рефакторинга и исправления кода, значительно упрощающих работу по написанию приложения;

− бесплатное распространение данного продукта.

# 4 Руководство пользователя

Для начала работы с данным приложением необходимо быть зарегистрированным в системе. Для запуска программы необходимо запустить исполняемый файл FMRD.exe. После запуска программы пользователю будет представлено диалоговое окно для авторизации в данном программном модуле. Данное диалоговое окно представлено на рисунке 4.1.

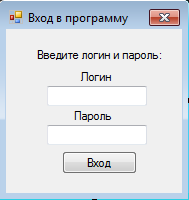


Рисунок 4.1 − Окно авторизации в программе

В случае ошибки авторизации программа выдаст сообщение о том что был введен неверный логин или пароль. В данном случае требуется закрыть окно с сообщением и заново ввести учетные данные. Пример сообщения показан на рисунке 4.2.

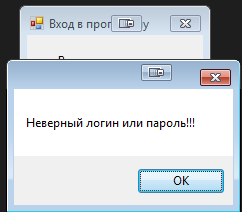


Рисунок 4.2 − Окно ошибки авторизации в программе

В случае успешного прохождения авторизации окно входа закроется и откроется главная форма приложения, представленная на рисунке 4.3.

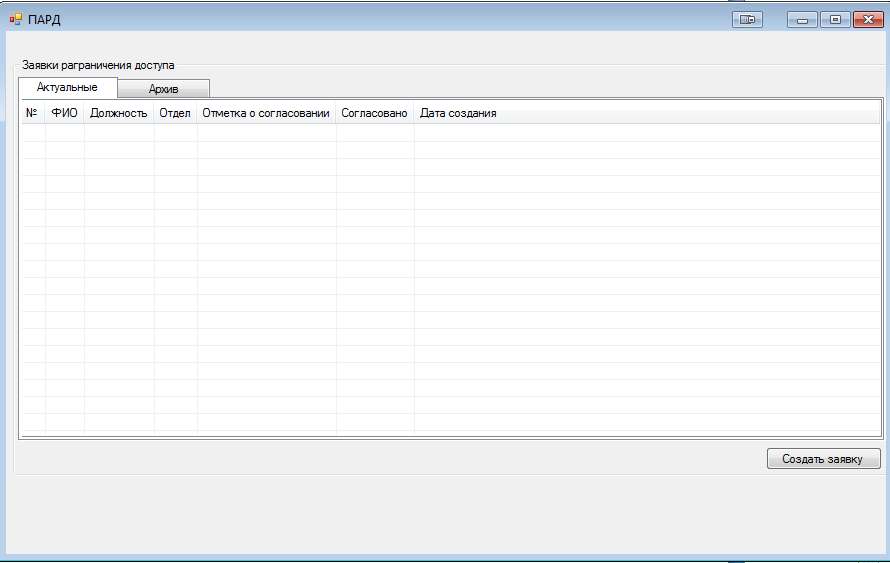


Рисунок 4.3 − Главная форма программного модуля

Главная форма содержит компонент вывода заявок и кнопку создания новых экземпляров заявок. Компонент вывода заявок состоит из двух вкладок, на которых расположены окна для вывода информации. На вкладке Актуальные содержатся созданные заявки, которые еще не обработаны администратором информационной системы. Отображается такая информация как номер заявки, фамилия имя отчество сотрудника, создавшего заявку, его должность в организации, наименование отдела и дату создания заявки. Также отображается информация о согласовании заявки с начальником отдела если необходимо. В данном случае отображается информация о отметке согласования и должность и инициалы человека, согласовавшего заявку. На вкладке архив отображаются заявки после обработки их администратором. На ней также имеется информация о создателе заявки, о согласовании и о дате создания заявки. Кроме данной информации, на вкладке также представлена данные администратора, который обработал заявку, дату обработки и результат. Вкладка Архив представлена на рисунке 4.4.

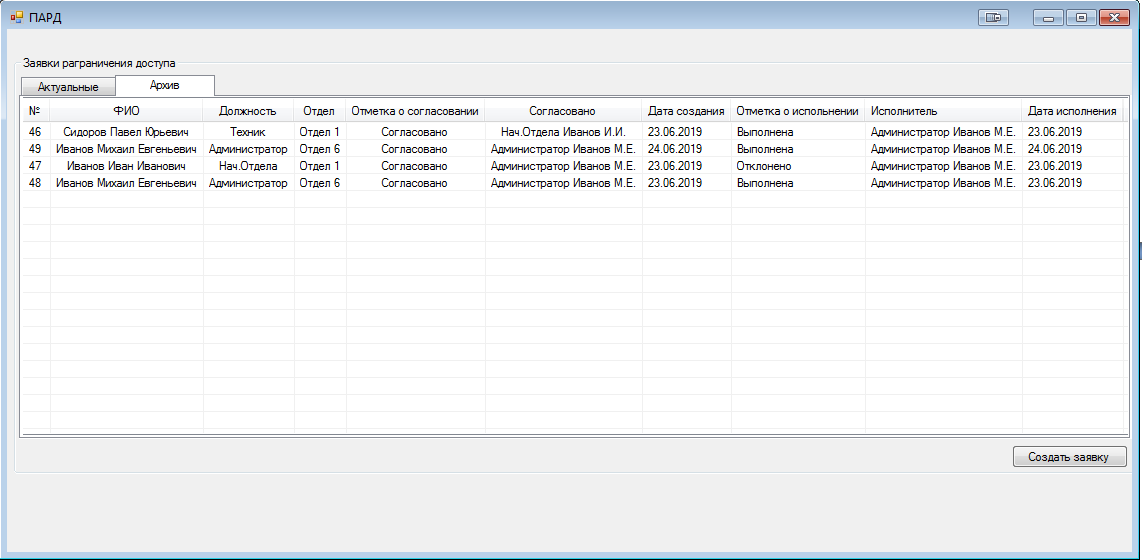


Рисунок 4.4 − Вкладка Архив

Для создания новой заявки на предоставление прав доступа пользователю необходимо нажать на кнопку Создать заявку. Данная кнопка содержится на главной форме программы под объектом для отображения заявок. Расположение кнопки представлено на рисунке 4.5.

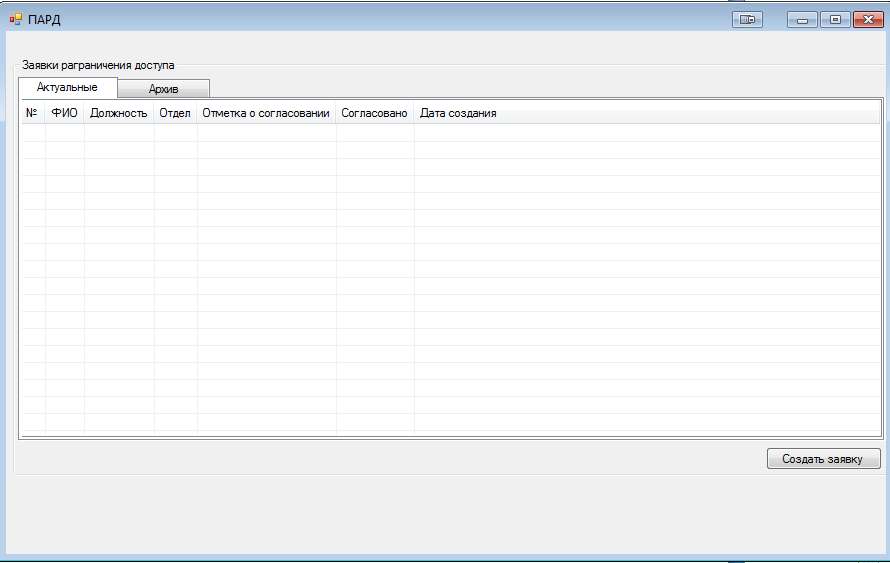


Рисунок 4.5 − Расположение кнопки создания заявки

После нажатия пользователем на кнопку создания заявки программа выведет на экран форму создания заявки. Данная форма представлена на рисунке 4.6.

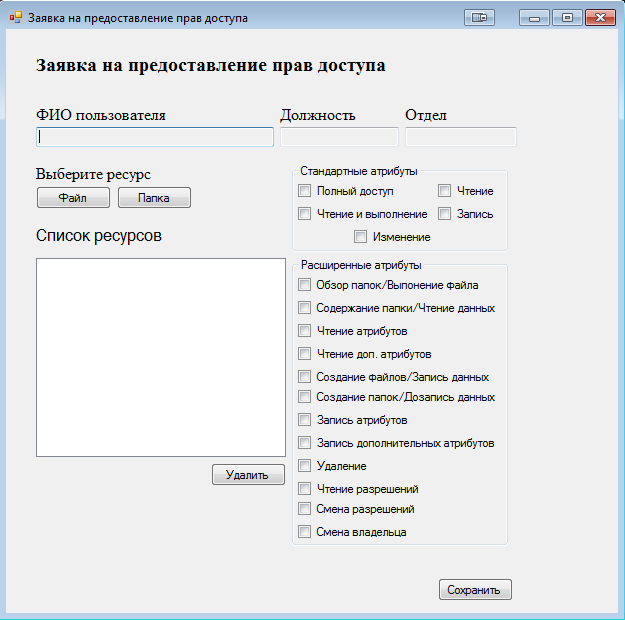


Рисунок 4.6 − Окно создания заявки предоставления доступа

В верхней части данной формы отображаются данные пользователя, на которого создается заявка предоставления доступа. В центре находится информация о ресурсах информационной системы к которым предоставляется доступ и права доступа. Правая часть окна с атрибутами прав доступа предназначена для просмотра назначенных прав доступа к определенному ресурсу. Создание заявки на предоставление прав доступа необходимо начать с заполнения данных о пользователе. Для этого пользователю необходимо совершить двойной щелчок правой кнопкой мыши по текстовому полю ФИО пользователя. После выполнения данного действия откроется окно выбора пользователя. Данное окно представлено на рисунке 4.7.

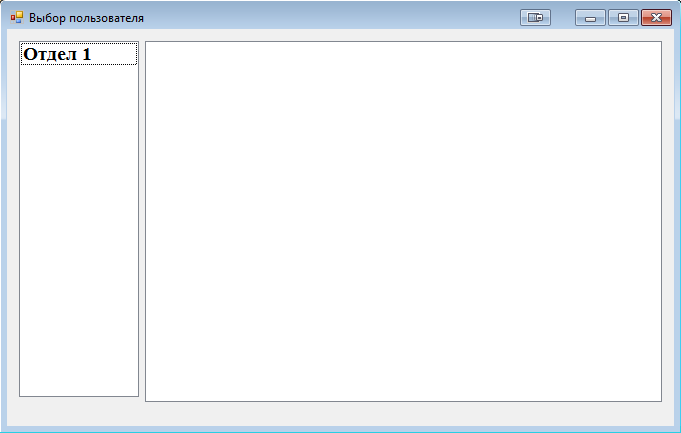


Рисунок 4.7 − Окно выбора пользователя

В левой части данной формы отображаются отделы, для работников которых можно создать заявку на предоставление доступа. Пользователь имеет право создавать заявки только для работников своего отдела. Для выбора отдела необходимо нажать левой кнопкой мыши на нужный отдел. После этого в правой части окна отобразятся доступные для выбора пользователи. В данной части отображается фамилия, имя, отчество работника, его занимаемая должность и отдел. Пример отображения пользователей показан на рисунке 4.8. Для выбора пользователя необходимо из предложенного списка выбрать пользователя и нажать на него двойным щелчком мыши. После выбора пользователя данные перенесутся на форму создания заявки, а данное окно закроется. В окне создания заявки на предоставления доступа в области данных о сотруднике в текстовых полях будут отображены данные о выбраном пользователе. Пример окна с отображением данных о выбранном пользователе показан на рисунке 4.9. После выбора пользователя, следующим шагом является выбор информационных ресурсов, к которым необходимо предоставить доступ.

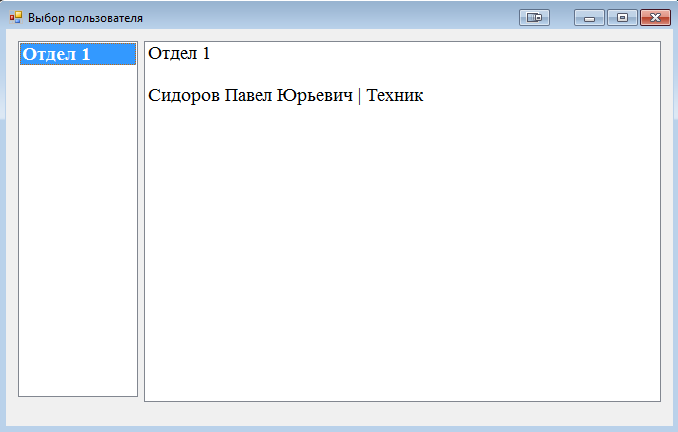


Рисунок 4.8 − Выбор пользователя для создания заявки

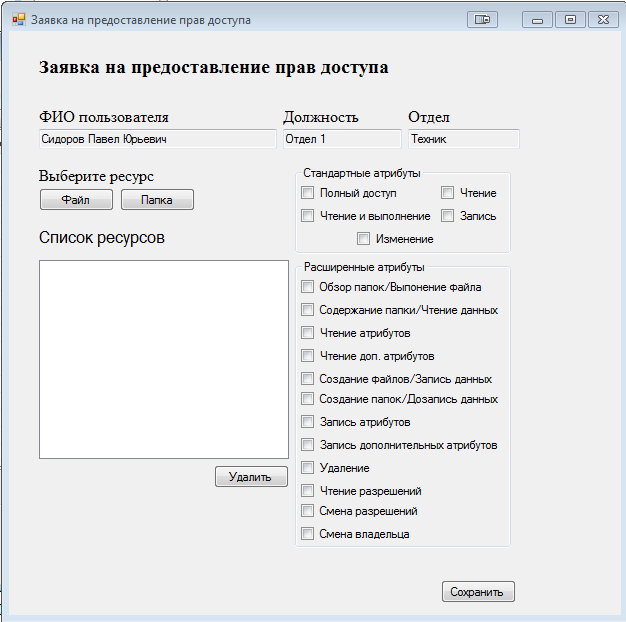


Рисунок 4.9 − Отображение выбранного пользователя

Для выбора информационных ресурсов предусмотрено две кнопки, одна из них с надписью Файл предназначена для добавления файлов в заявку, вторая с надписью Папка предназначена для добавления в заявку папки. Расположение данных элементов управления показано на рисунке 4.10.

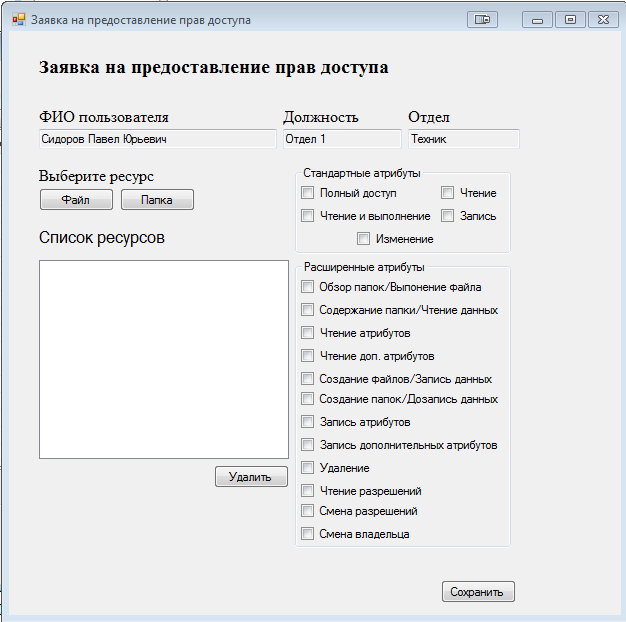


Рисунок 4.10 − Элементы управления для добавления ресурсов

При выборе файла откроется диалоговое окно, в котором пользователю необходимо выбрать нужный файл. Диалоговое окно представлено на рисунке 4.11.

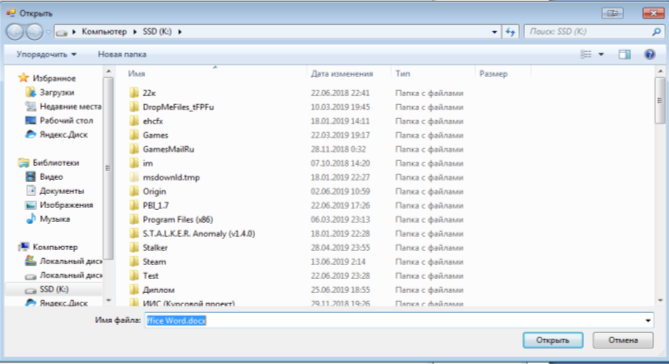


Рисунок 4.11 − Диалоговое окно выбора файла

При выборе папки откроется диалоговое окно, в котором пользователю необходимо выбрать нужную папку. Диалоговое окно представлено на рисунке 4.12.

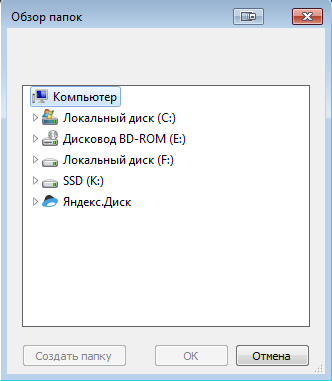


Рисунок 4.12 − Диалоговое окно выбора папки

После выбора ресурсов, они добавляются в область окна Список ресурсов. Файлы выделены синим значком файла, а папки черным значком папки соответственно. Список ресурсов показан на рисунке 4.13.

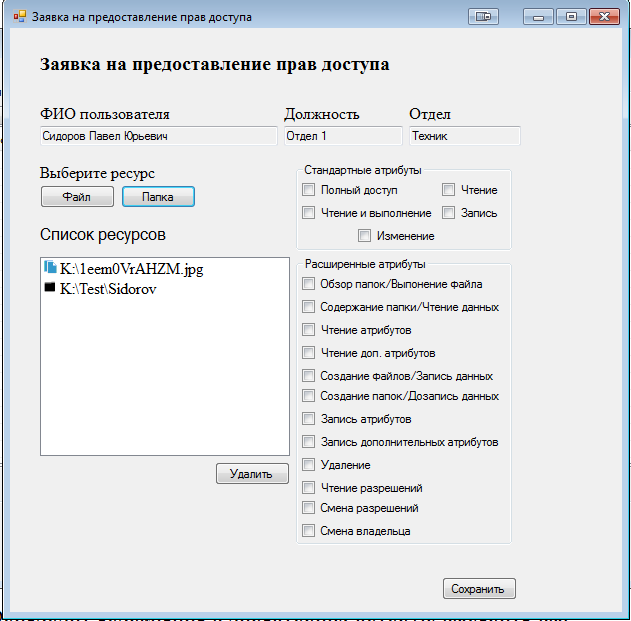


Рисунок 4.13 − Список выбранных ресурсов

Обратите внимание что при выборе ресурсов текстовые поля с данными пользователя становятся неактивны. Дальнейшим действием пользователя является выбор прав доступа для каждого ресурса из списка ресурсов. Для открытия окна для выбора прав доступа пользователю необходимо сделать двойной щелчок мыши по выбранному ресурсу. Пользователь перейдет в окно настройки прав доступа. Данное окно представлено на рисунке 4.14.

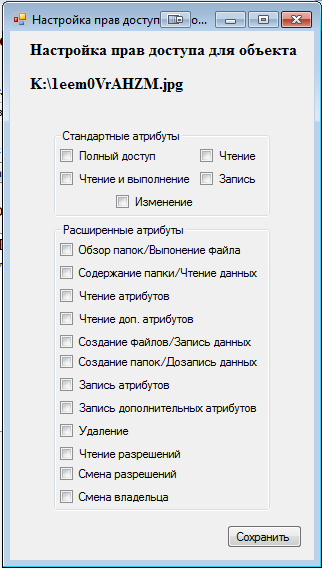


Рисунок 4.14 − Окно настройки прав доступа

На данном окне происходит назначение прав доступа. Для назначения требуемых прав пользователю необходимо произвести их выбор путем нажатия на соответствующее право. Права делятся на два списка, стандартные атрибуты и расширенные. Стандартные атрибуты представляют собой объединение нескольких расширенных атрибутов, например стандартный атрибут чтение содержит в себе права чтение атрибутов, чтение доп. атрибутов, чтение данных и чтение разрешений. При выборе прав доступа советуется настраивать только права в одном из списков. Заполненное окно прав показано на рисунке 4.15.

После выбора всех необходимых прав доступа пользователю необходимо сохранить внесенные изменения. Для этого необходимо нажать на кнопку сохранить в нижней части окна.

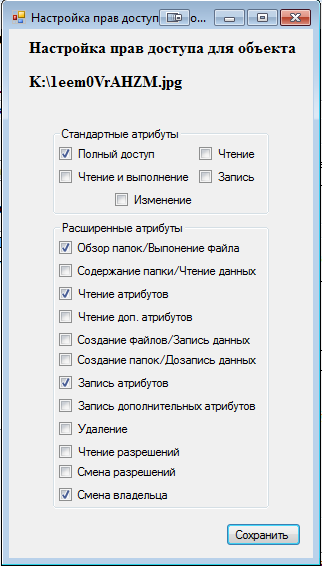


Рисунок 4.15 − Заполненное окно прав доступа к ресурсу

Программа выведет сообщение о том что сохранение успешно. После сохранения данное окно закроется, пользователь перейдет на форму создания заявки. Выбранные права доступа будут отображаться справа от списка ресурсов. Можно просмотреть права у всех выбранных ресурсов выбирая их левой кнопкой мыши. Изменение прав доступа на данной форме недоступно, данная часть окна предназначена только для просмотра прав. Пример отображения заполненных прав доступа к ресурсу представлен на рисунке 4.16.

По аналогии с описанным выше, пользователю необходимо настроить права доступа для всех выбранных ресурсов. В случае необходимости пользователь может удалять ресурсы из списка. Для этого необходимо выбрать нужный ресурс и нажать кнопку Удалить. Ресурс удалиться из списка ресурсов, также удалятся и права доступа, если пользователь их настраивал.

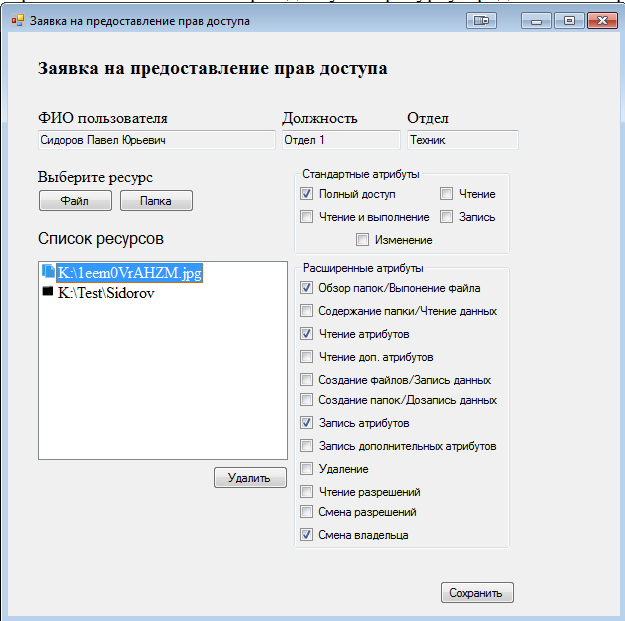


Рисунок 4.16 − Отображение прав в окне создания заявки

После заполнения прав доступа для всех выбранных ресурсов необходимо сформировать и сохранить данную заявку. Для этого пользователю необходимо нажать на кнопку Сохранить. Если сохранение прошло успешно, программа выведет сообщение о том что сохранение успешно. Данное сообщение представлено на рисунке 4.17. После сохранения заявки, пользователь возвращается на главную форму приложения. При необходимости пользователь может заново произвести процесс создания новой заявки на предоставление доступа. Созданные заявки отображаются на главной форме на вкладке актуальные. В данной вкладке содержатся данные о создателе заявки, его фамилия, имя, отчество, должность и отдел, и дата создания заявки. Исполнением заявок занимается администратор информационной системы. Также на главной форме есть данные о согласовании. Согласование необходимо для подтверждения заявки начальником отдела. Отображение заявки на главной форме приложения показано на рисунке 4.18.

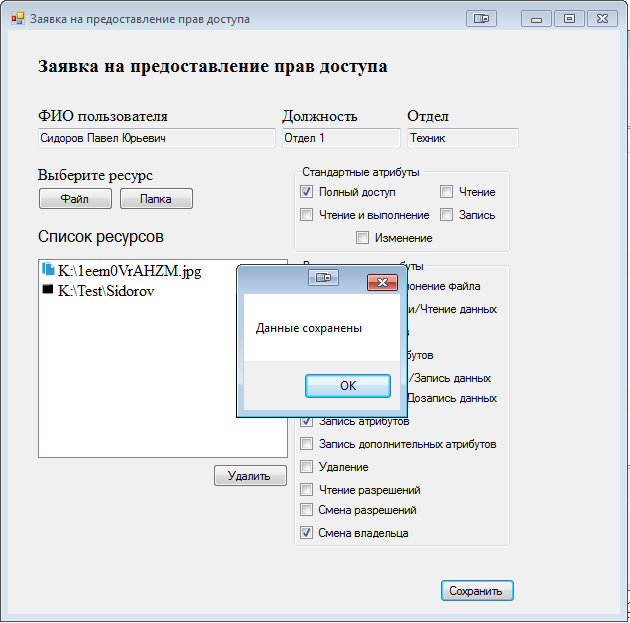


Рисунок 4.17 − Сохранение созданной заявки

Если пользователь является начальником отдела, то данный пользователь на главной форме видит все заявки, которые создавали работники его отдела. Начальник отдела имеет право просматривать все созданные заявки в своем отделе и при необходимости ставить отметку о согласовании. Начальник отдела не имеет прав на редактирование созданной заявки. В случае если начальник отдела не согласен с содержимым созданной заявки, то он может ее отклонить. В таком случае заявка будет отображаться на вкладке Архив. Пример отображения согласованной заявки показан на рисунке 4.19.

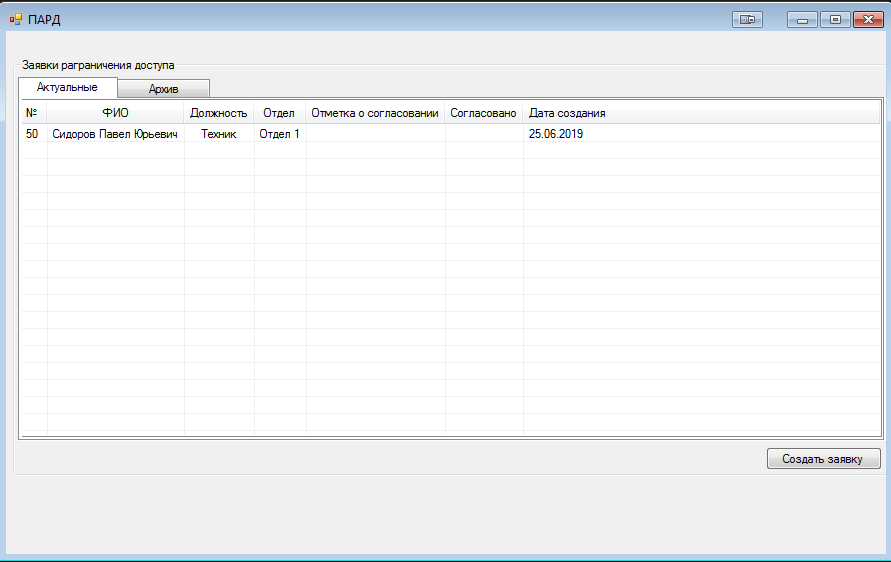


Рисунок 4.18 − Отображение созданной заявки на главном окне

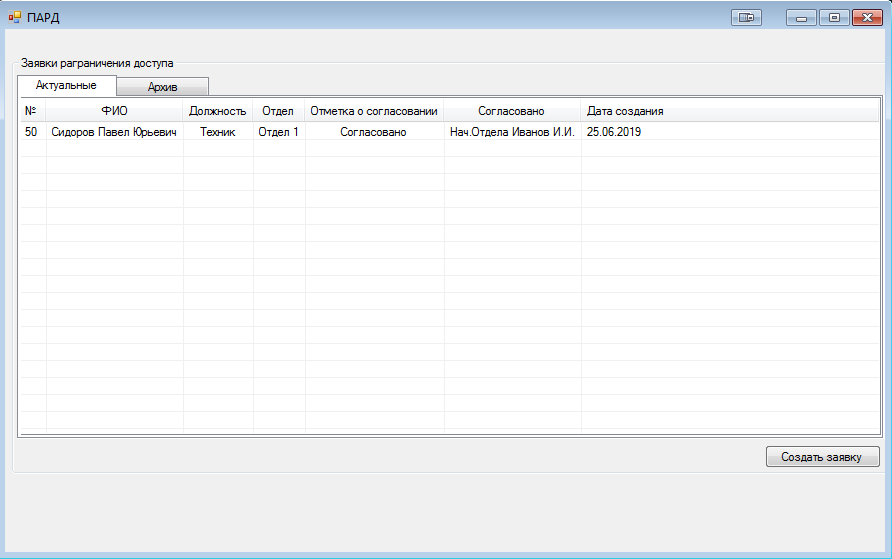


Рисунок 4.19 − Отображение согласованной заявки на главном окне

На рисунке 4.20 показано окно просмотра созданной заявки начальником отдела и элементы управления согласованием.

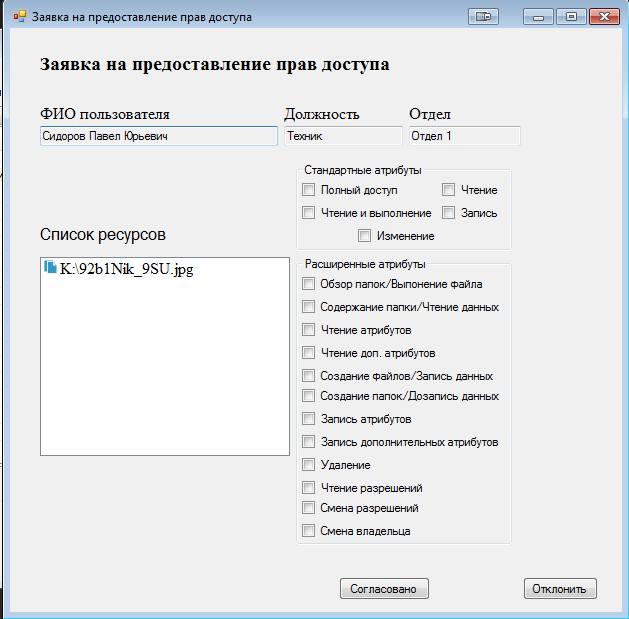


Рисунок 4.20 − Просмотр заявки с возможностью согласования

Начальник отдела также имеет права для создания заявок на каждого работника его отдела. В окне выбора пользователя для него отображаются все работники, которые числятся в его отделе.

# 5 Руководство администратора

Для начала работы с данным приложением необходимо быть зарегистрированным в системе. Для запуска программы необходимо запустить исполняемый файл FMRD.exe. После запуска программы администратору будет представлено диалоговое окно для авторизации в данном программном модуле. Данное диалоговое окно представлено на рисунке 5.1.

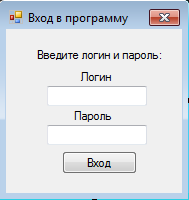


Рисунок 5.1 − Окно авторизации в программе

В случае ошибки авторизации программа выдаст сообщение о том что был введен неверный логин или пароль. В данном случае требуется закрыть окно с сообщением и заново ввести учетные данные. Пример сообщения показан на рисунке 5.2.

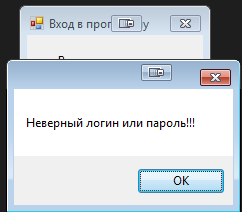


Рисунок 5.2 − Окно ошибки авторизации в программе

В случае успешного прохождения авторизации окно входа закроется и откроется главная форма приложения, представленная на рисунке 5.3.

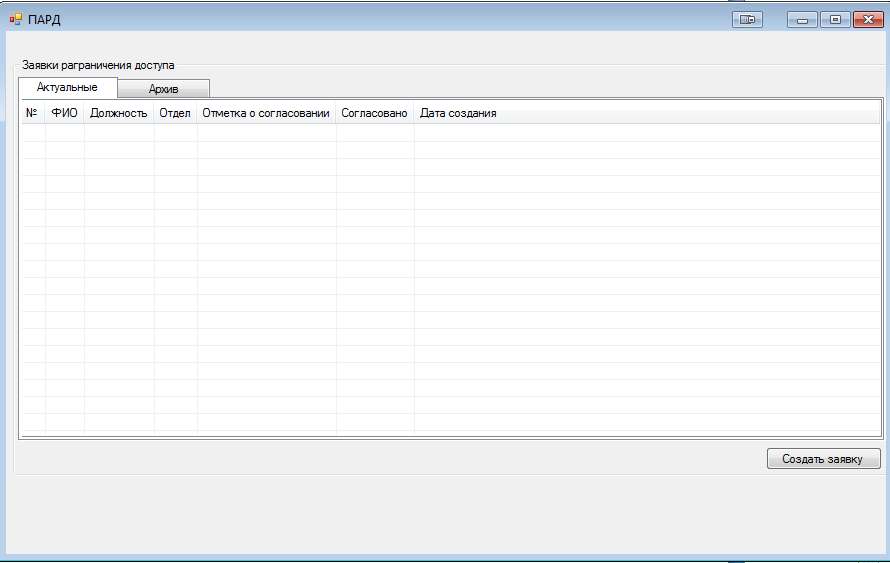


Рисунок 5.3 − Главная форма программного модуля

Главная форма содержит компонент вывода заявок и кнопку создания новых экземпляров заявок. Компонент вывода заявок состоит из двух вкладок, на которых расположены окна для вывода информации. На вкладке Актуальные содержатся созданные заявки, которые еще не обработаны администратором информационной системы. Отображается такая информация как номер заявки, фамилия имя отчество сотрудника, создавшего заявку, его должность в организации, наименование отдела и дату создания заявки. Также отображается информация о согласовании заявки с начальником отдела если необходимо. В данном случае отображается информация о отметке согласования и должность и инициалы человека, согласовавшего заявку. На вкладке архив отображаются заявки после обработки их администратором. На ней также имеется информация о создателе заявки, о согласовании и о дате создания заявки. Кроме данной информации, на вкладке также представлена данные администратора, который обработал заявку, дату обработки и результат. Вкладка Архив представлена на рисунке 5.4.

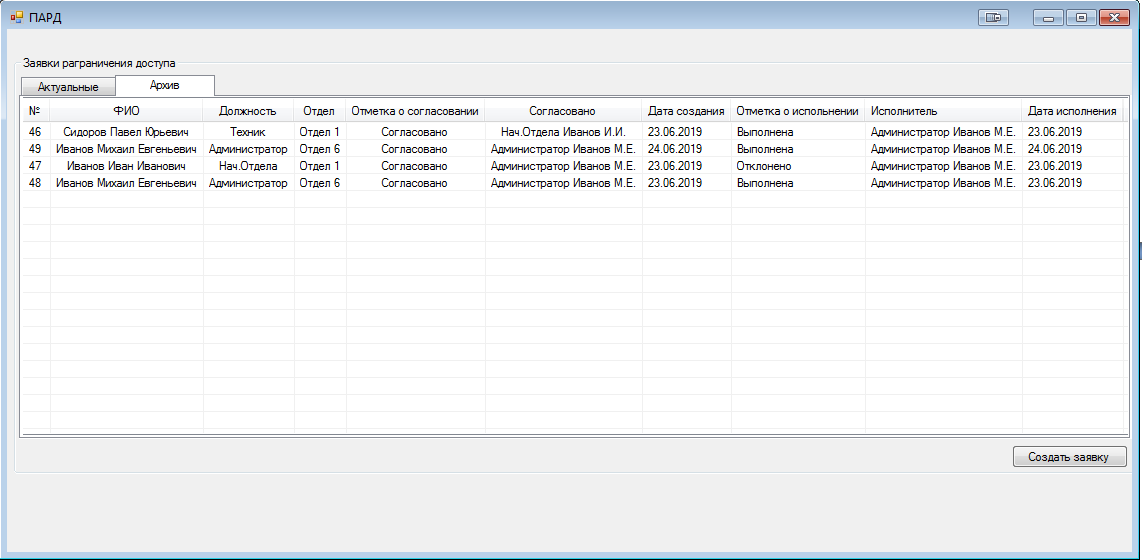


Рисунок 5.4 − Вкладка Архив

Для создания новой заявки на предоставление прав доступа администратору необходимо нажать на кнопку Создать заявку. Данная кнопка содержится на главной форме программы под объектом для отображения заявок. Расположение кнопки представлено на рисунке 5.5.

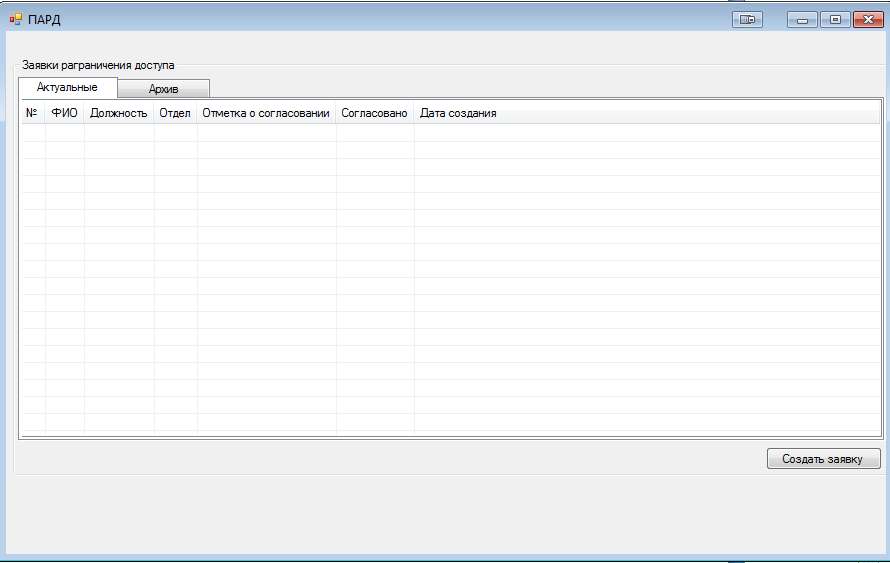


Рисунок 5.5 − Расположение кнопки создания заявки

После нажатия администратором на кнопку создания заявки программа выведет на экран форму создания заявки. Данная форма представлена на рисунке 5.4.

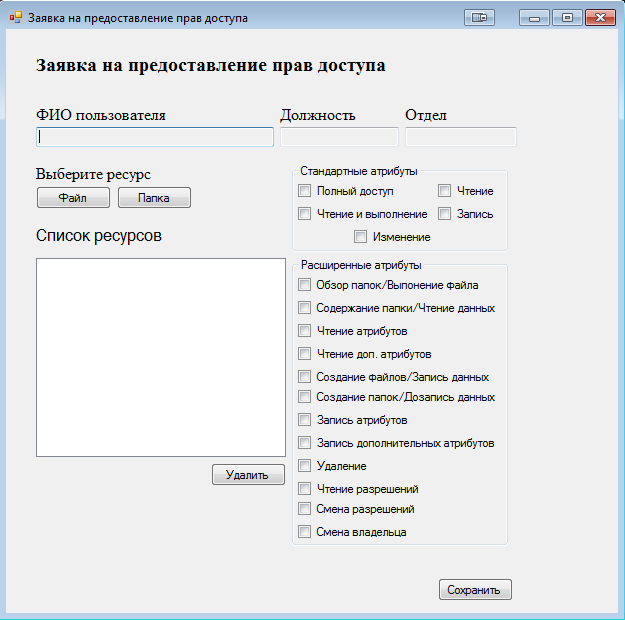


Рисунок 5.6 − Окно создания заявки предоставления доступа

В верхней части данной формы отображаются данные пользователя, на которого создается заявка предоставления доступа. В центре находится информация о ресурсах информационной системы к которым предоставляется доступ и права доступа. Правая часть окна с атрибутами прав доступа предназначена для просмотра назначенных прав доступа к определенному ресурсу. Создание заявки на предоставление прав доступа необходимо начать с заполнения данных о пользователе. Для этого администратору необходимо совершить двойной щелчок правой кнопкой мыши по текстовому полю ФИО пользователя. После выполнения данного действия откроется окно выбора пользователя. Данное окно представлено на рисунке 5.7.

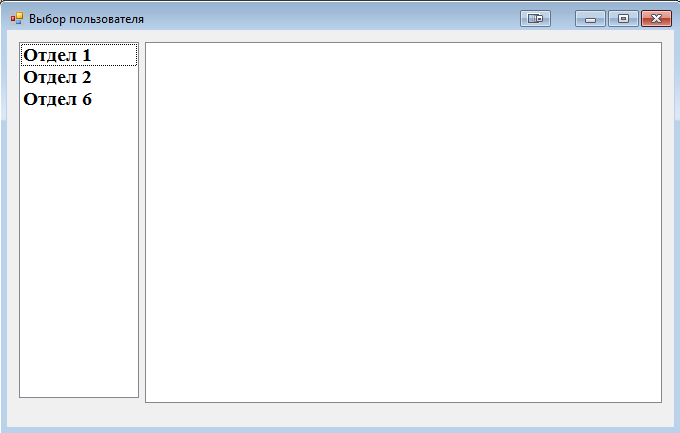


Рисунок 5.7 − Окно выбора пользователя

В левой части данной формы отображаются отделы, для работников которых можно создать заявку на предоставление доступа. Администратор имеет право создавать заявки для работников всей организации. Для выбора отдела необходимо нажать левой кнопкой мыши на нужный отдел. После этого в правой части окна отобразятся доступные для выбора пользователи. В данной части отображается фамилия, имя, отчество работника, его занимаемая должность и отдел. Пример отображения пользователей показан на рисунке 5.8. Для выбора пользователя необходимо из предложенного списка выбрать пользователя и нажать на него двойным щелчком мыши. После выбора пользователя данные перенесутся на форму создания заявки, а данное окно закроется. В окне создания заявки на предоставления доступа в области данных о сотруднике в текстовых полях будут отображены данные о выбранном пользователе. Пример окна с отображением данных о выбранном пользователе показан на рисунке 5.9. После выбора пользователя, следующим шагом является выбор информационных ресурсов, к которым необходимо предоставить доступ.

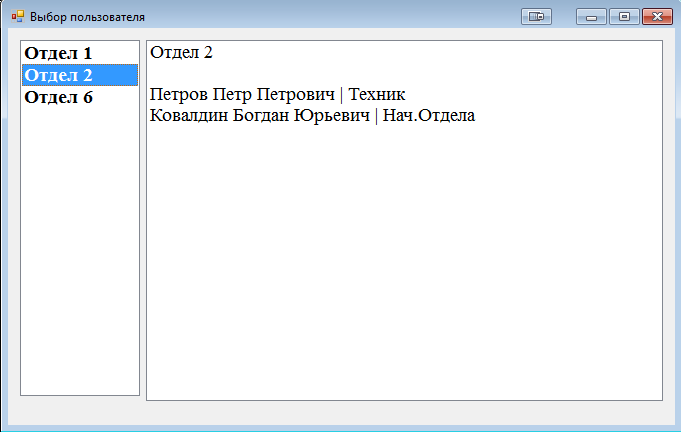


Рисунок 5.8 − Выбор пользователя для создания заявки

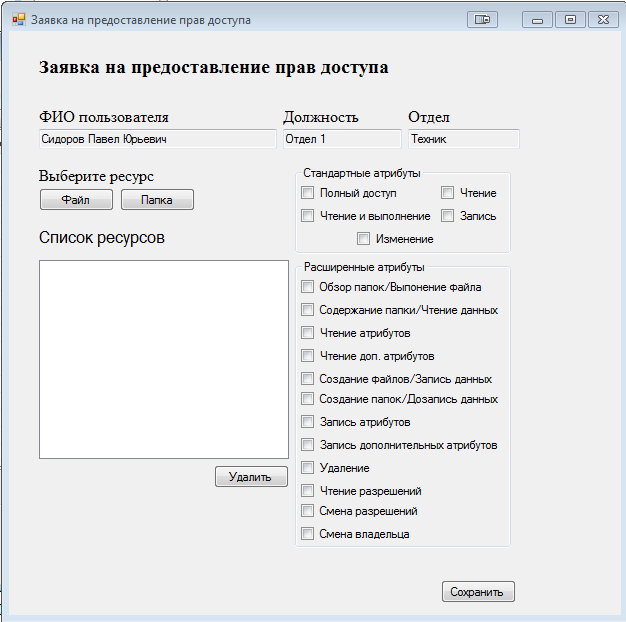


Рисунок 5.9 − Отображение выбранного пользователя

Для выбора информационных ресурсов предусмотрено две кнопки, одна из них с надписью Файл предназначена для добавления файлов в заявку, вторая с надписью Папка предназначена для добавления в заявку папки. Расположение данных элементов управления показано на рисунке 5.10.

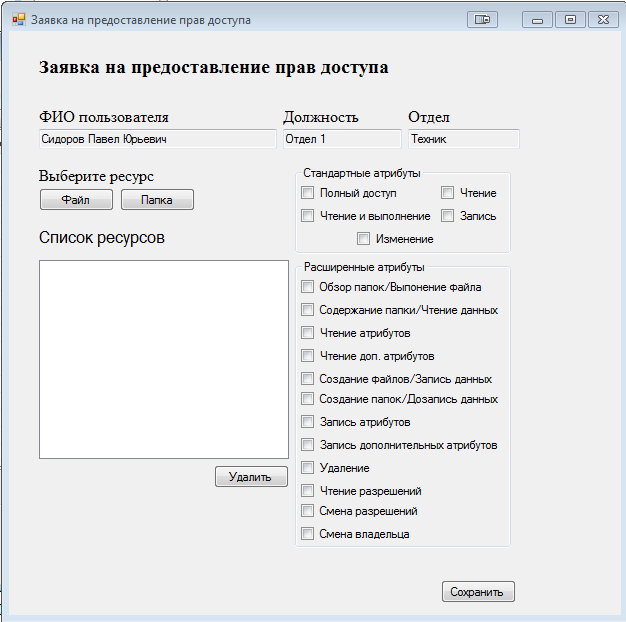


Рисунок 5.10 − Элементы управления для добавления ресурсов

При выборе файла откроется диалоговое окно, в котором администратору необходимо выбрать нужный файл. Диалоговое окно представлено на рисунке 5.11.

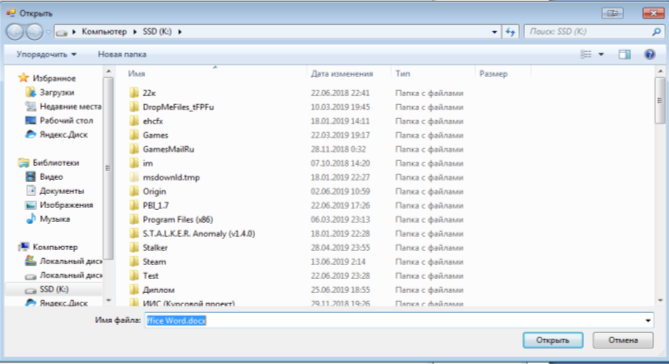


Рисунок 5.11 − Диалоговое окно выбора файла

При выборе папки откроется диалоговое окно, в котором администратору необходимо выбрать нужную папку. Диалоговое окно представлено на рисунке 5.12.

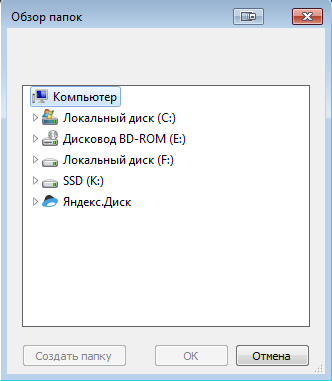


Рисунок 5.12 − Диалоговое окно выбора папки

После выбора ресурсов, они добавляются в область окна Список ресурсов. Файлы выделены синим значком файла, а папки черным значком папки соответственно. Список ресурсов показан на рисунке 5.13.

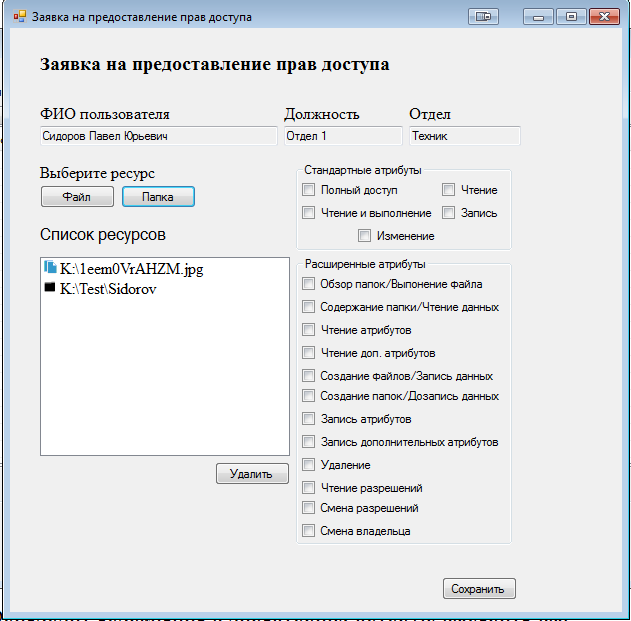


Рисунок 5.13 − Список выбранных ресурсов

Обратите внимание что при выборе ресурсов текстовые поля с данными пользователя становятся неактивны. Дальнейшим действием пользователя является выбор прав доступа для каждого ресурса из списка ресурсов. Для открытия окна для выбора прав доступа пользователю необходимо сделать двойной щелчок мыши по выбранному ресурсу. Администратор перейдет в окно настройки прав доступа. Данное окно представлено на рисунке 5.14.

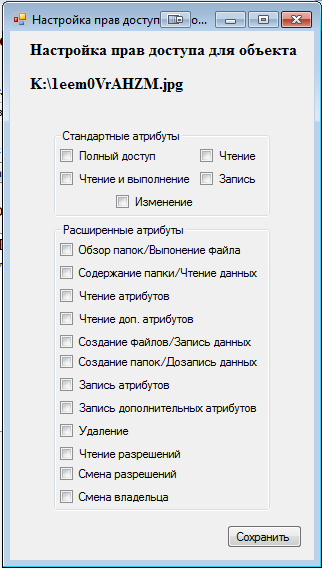


Рисунок 5.14 − Окно настройки прав доступа

На данном окне происходит назначение прав доступа. Для назначения требуемых прав пользователю необходимо произвести их выбор путем нажатия на соответствующее право. Права делятся на два списка, стандартные атрибуты и расширенные. Стандартные атрибуты представляют собой объединение нескольких расширенных атрибутов, например стандартный атрибут чтение содержит в себе права чтение атрибутов, чтение доп. атрибутов, чтение данных и чтение разрешений. При выборе прав доступа советуется настраивать только права в одном из списков. Заполненное окно прав показано на рисунке 5.15.

После выбора всех необходимых прав доступа администратору необходимо сохранить внесенные изменения. Для этого необходимо нажать на кнопку сохранить в нижней части окна.

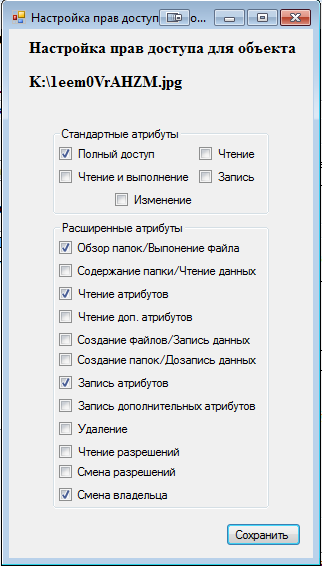


Рисунок 5.15 − Заполненное окно прав доступа к ресурсу

Программа выведет сообщение о том что сохранение успешно. После сохранения данное окно закроется, администратор перейдет на форму создания заявки. Выбранные права доступа будут отображаться справа от списка ресурсов. Можно просмотреть права у всех выбранных ресурсов выбирая их левой кнопкой мыши. Изменение прав доступа на данной форме недоступно, данная часть окна предназначена только для просмотра прав. Пример отображения заполненных прав доступа к ресурсу представлен на рисунке 5.14.

По аналогии с описанным выше, администратору необходимо настроить права доступа для всех выбранных ресурсов. В случае необходимости администратор может удалять ресурсы из списка. Для этого необходимо выбрать нужный ресурс и нажать кнопку Удалить. Ресурс удалиться из списка ресурсов, также удалятся и права доступа, если администратор их настраивал.

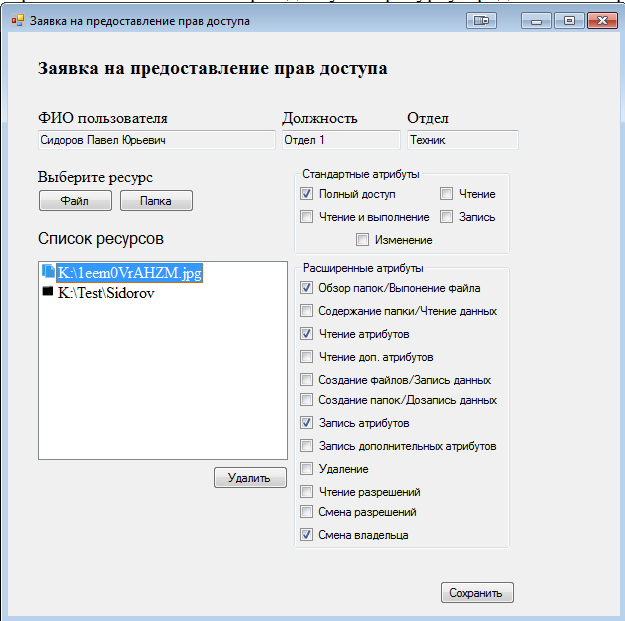


Рисунок 5.16 − Отображение прав в окне создания заявки

После заполнения прав доступа для всех выбранных ресурсов необходимо сформировать и сохранить данную заявку. Для этого администратору необходимо нажать на кнопку Сохранить. Если сохранение прошло успешно, программа выведет сообщение о том что сохранение успешно. Данное сообщение представлено на рисунке 5.17. После сохранения заявки, администратор возвращается на главную форму приложения. При необходимости администратор может заново произвести процесс создания новой заявки на предоставление доступа. Созданные заявки отображаются на главной форме на вкладке актуальные. В данной вкладке содержатся данные о создателе заявки, его фамилия, имя, отчество, должность и отдел, и дата создания заявки. Исполнением заявок занимается администратор информационной системы. Также на главной форме есть данные о согласовании. Согласование необходимо для подтверждения заявки начальником отдела. Отображение заявки на главной форме приложения показано на рисунке 5.18.

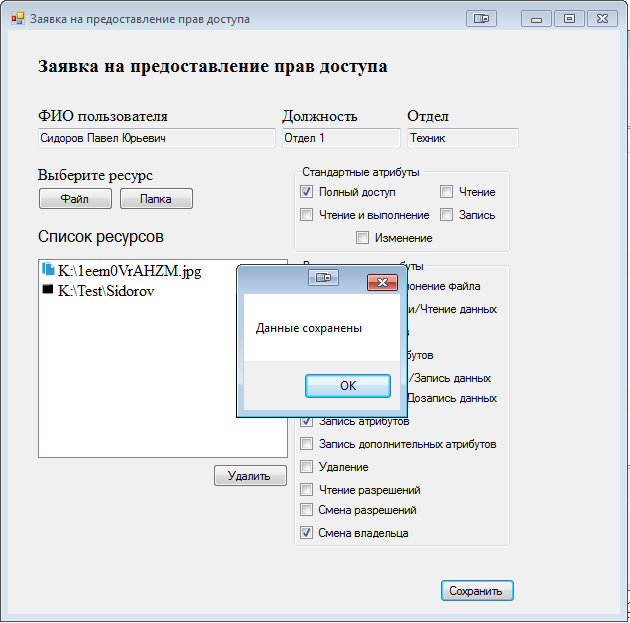


Рисунок 5.17 − Сохранение созданной заявки

Администратор, также как и начальник отдела, на главной форме видит все заявки, но которые создавали работники всей организации. Администратор отдела имеет право просматривать все созданные заявки и при необходимости ставить отметку о согласовании. Администратор не имеет прав на редактирование созданной заявки. В случае если администратор не согласен с содержимым созданной заявки, то он может ее отклонить. В таком случае заявка будет отображаться на вкладке Архив. Пример отображения согласованной заявки показан на рисунке 5.19.

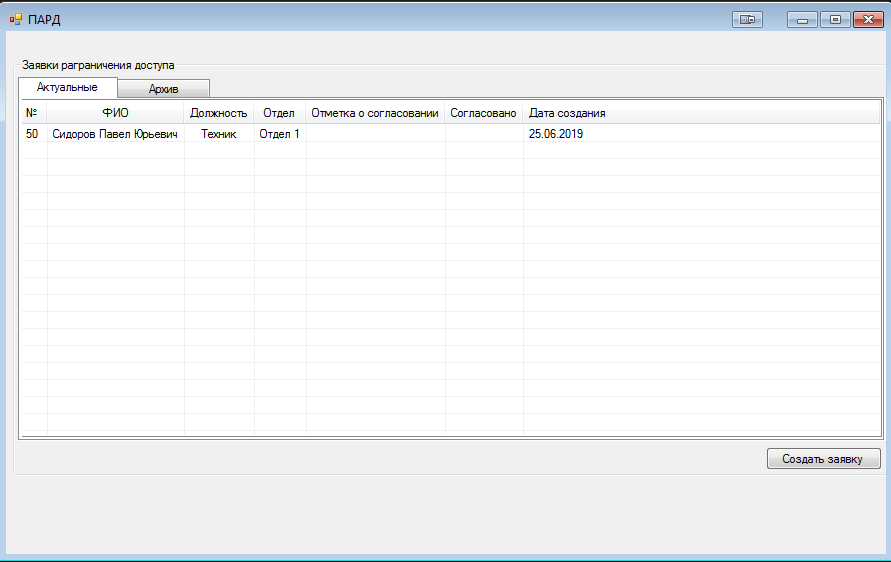


Рисунок 5.18 − Отображение созданной заявки на главном окне

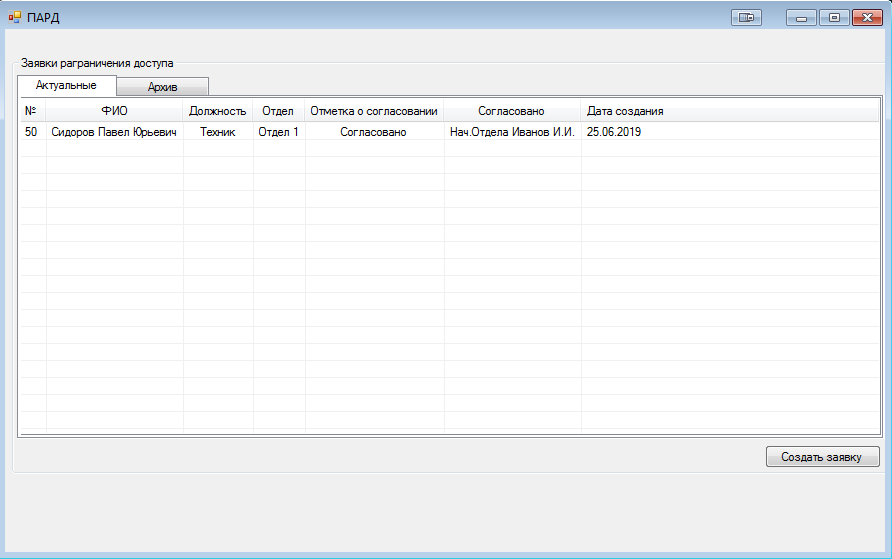


Рисунок 5.19 − Отображение согласованной заявки на главном окне

На рисунке 5.20 показано окно просмотра созданной заявки администратором и элементы управления заявкой.

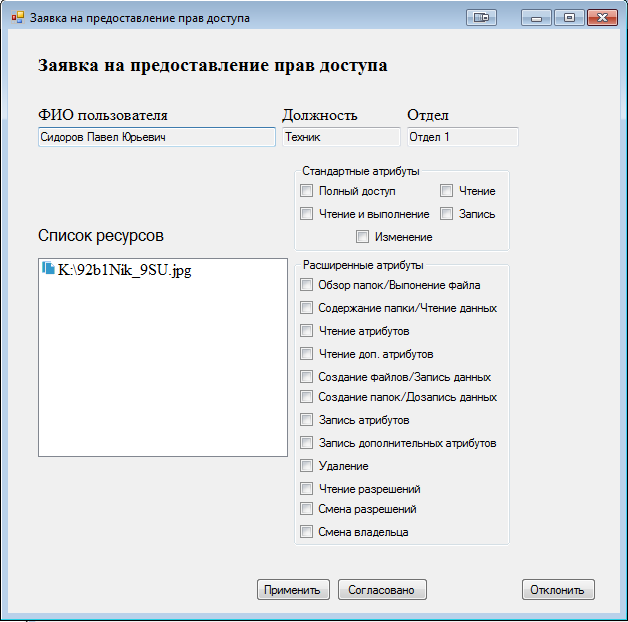


Рисунок 5.20 − Просмотр заявки с правами администратора

Кроме возможности согласования и отклонения заявки на этапе согласования, администратор имеет функционал для отмены уже согласованных заявок.

Главным инструментом администратора является возможность применять права доступа из созданных заявок. Для этого администратору необходимо в открытой заявке нажать кнопку применить. Программа автоматически считывает все данные о пользователях, информационных ресурсах и правах доступа и применяет их к информационной системе. После успешного применения прав доступа программа выведет сообщение об окончании настройки. Пример сообщения показан на рисунке 5.21.

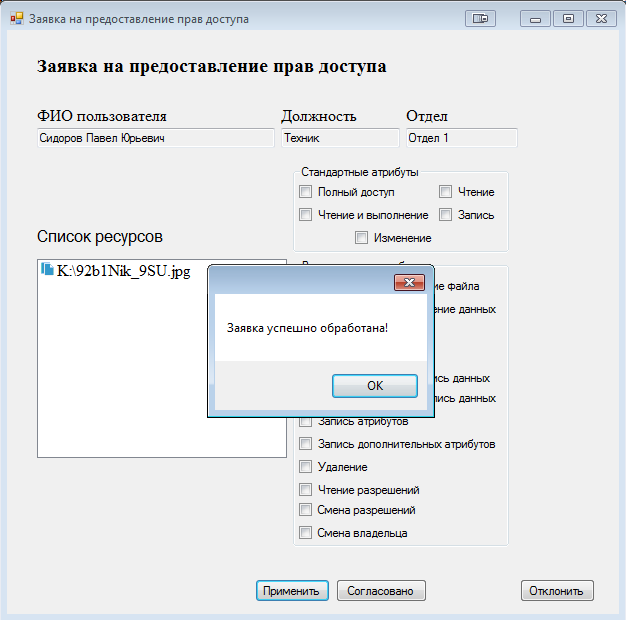


Рисунок 5.21 − Применение заявки в информационной системе

Администратор также имеет права на создание заявок на каждого работника организации. В окне выбора пользователя для него отображаются все отделы и пользователи, которые числятся в организации.

# Заключение

Результатом выполнения научно-исследовательской работы стало создание прототипа программного средства для реализации автоматизации настройки дискреционного метода разграничения доступа в информационной системе предприятия.

Данное приложение разработано под операционную систему Windows 7 и использует стандартные средства разграничения доступа данной операционной системы. В данной работе был реализован дискреционный метод разграничения доступа, как самый трудозатратный в применении.

Реализован процесс создания запросов на разграничения доступа в виде электронных заявок. Для ускорения процесса формирования запроса, возможность создавать заявки получили все пользователи информационной системы. Также были введены промежуточные узлы между составителем и исполнителем заявки для согласования, а за счет использования базы данных значительно возросла скорость передачи заявки исполнителю и ее обработка.

Программный продукт существенно упростил использование стандартных средств операционной системы Windows для разграничения доступа в небольших организациях и в некоторых случаях позволяет обойтись без привлечения специалистов.

В данной работе показаны основные функции, позволяющие упростить процесс настройки доступа. Для использования в организации программа может быть дополнена для выполнения определенных целей, например программа может быть дополнена другими методами разграничения доступа.

Список используемых источников

1. Анисимов, В.В. Проектирование информационных систем: курс лекций [Электронный ресурс] – Режим доступа: https://sites.google.com/site/anisimovkhv/learning/pris/lecture/
2. Щеглов, А. Ю. Защита компьютерной информации от несанкционированного доступа/ А.Ю. Щеглов–СПб.: НиТ–Петербург, 2004–384с
3. Википедия. Свободная энциклопедия [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/
4. MSDN[Электронныйресурс]: Сеть разработчиков Microsoft–Электрон. журн. – М.: Майкрософт –Режим доступа:https://msdn.microsoft.com/ru/
5. StackOverflow [Электронный ресурс] / Сайт вопросов и ответов для программистов. –Режим доступа: http://stackoverflow.com
6. CyberForum.ru [Электронный ресурс] / Форум программистов и сисадминов. – Режим доступа: http://www.cyberforum.ru
7. Меры защиты информации в государственных информационных системах [Текст] : методический документ : [утв. ФСТЭК России 11 февраля 2014г. ].
8. Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных [Текст] : приказ ФСТЭК России от 18 февраля 2013 г. №21 // Российская газета. − 2013г. − №107, 22 мая.
9. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности ISO/IEC 27002 [Текст] : Утвержден и введен в действие приказом федерального агентства по техническому регулированию и метрологии от 24 сентября 2012 г. № 423–ст.

10. О персональных данных [Текст] : федер. закон : [принят Гос. Думой 8 июля 2006 г. № 152–ФЗ : одобр. Советом Федерации 14 июля 2006 г.]. − М.: Ось–98, [2006г.].

11. CLR via C#. Программирование на платформе Microsoft .NET Framework 4.5 на языке C#, 4–е изд. Дж. Рихтер.

12. Международный стандарт по информационной безопасности ISO/IEC 27001 [Текст] : Утвержден и введен в действие приказом Федерального агентства по регулированию и метрологии от 27 декабря 2006 г. № 375–ст.

13. Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах [Текст] : приказ ФСТЭК России от 11 февраля 2013г. №17 // Российская газета. − 2013г. − №1136, 26 июня.

14. Гайдамакин, Н. А. Разграничение доступа к информации в компьютерных системах:Учеб. пособие / Н. А. Гайдамакин. - Екатеринбург: изд-во Урал. Ун-та, 2003. – 328 с.

15. Гайдамакин, Н.А. Теоретические основы компьютерной безопасности: Учеб. пособие /Н. А. Гайдамакин. - Екатеринбург: изд-во Урал. Ун-та, 2008. – 212 с.

16. Девянин П. Н. Модели безопасности компьютерных систем: Учеб. пособие / П. Н. Девянин. – М.: Изд.центр «Академия», 2005. – 144 с.

# Основные определения

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора (подтверждение подлинности субъекта доступа в информационной системе).

Доступ к информации, составляющей коммерческую тайну, – ознакомление определенных лиц с информацией, составляющей коммерческую тайну, с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации.

Идентификация – присвоение субъектам доступа, объектам доступа идентификаторов (уникальных имен) и (или) сравнение предъявленного идентификатора с перечнем присвоенных идентификаторов.

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Информация, составляющая коммерческую тайну, – сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно–технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны.

Коммерческая тайна – режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

Обладатель информации, составляющей коммерческую тайну, – лицо, которое владеет информацией, составляющей коммерческую тайну, на законном основании, ограничило доступ к этой информации и установило в отношении ее режим коммерческой тайны.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Объект доступа – единица информативного ресурса информационной системы (файл, техническое средство, узел сети, линия (канал) связи, мобильное устройство, программа, том, каталог, запись и иные объекты), доступ к которой регламентируется правилами разграничения доступа и по отношению к которой субъекты доступа выполняют операции.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Пользователь – лицо, которому разрешено выполнять некоторые действия (операции) по обработке информации в информационной системе или использующее результаты ее функционирования.

Субъект доступа – пользователь, процесс, выполняющий операции (действия) над объектами доступа и действия которых регламентируются правилами разграничения доступа.

Управление доступом – ограничение и контроль доступа субъектов доступа к объектам доступа в информационной системе в соответствии с установленными правилами разграничения доступа.