МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»

Институт математики, физики и информационных технологий
(наименование института полностью)

Кафедра «Прикладная математика и информатика»
(наименование)

09.04.03 Прикладная информатика
(код и наименование направления подготовки)

Информационные системы и технологии корпоративного управления
(направленность (профиль))

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ)

на тему «Методы и технологии организации доступа к информационным корпоративным ресурсам»

Студент К.И. Проскурняк
(И.О. Фамилия) (личная подпись)

Научный руководитель к.пед.н. О.Ю. Копша
(ученая степень, звание, И.О. Фамилия)

Тольятти 2021

Оглавление

Введение

Актуальность работы: на основании менеджмента ООО «ИЦ АЙ-ТЕКО» можно приравнивать к категории комплексных и охарактеризовать, как, имеющую множество уровней и являющейся географически многоуровневой и географически организованной структурой.

ООО «ИЦ АЙ-ТЕКО» использует свободный спектр систем автоматизирования бизнеса: ERP, SCADA, MES, CRM и др.

Интегрированная система ООО «ИЦ АЙ-ТЕКО» иерархически сложно выстроена. Диспетчерские службы и производственные подразделения в ней административно зависимы.

Создаётся и используется большое количество информационных источников различной степени конфиденциальности в процессе работы ООО «ИЦ АЙ-ТЕКО».

С точки зрения архитектуры введения автоматизированной системы управления ООО «ИЦ АЙ-ТЕКО», наиболее действенным, считается корпоративный портал, какой обязан быть интегрированным веб-приложением класса B2E, которое может обеспечить юзерам единственную точку перекрестного доступа к назначенной для них разделенной ИР.

Перекрестный доступ подлежит взаимному использованию информационных систем (ИС) разнообразными подразделениями ООО «ИЦ АЙ-ТЕКО» и их партнерами в отсутствие каких-либо нарушений конфиденциальности.

Сложность определения основных принципов управления доступом к информационным ресурсам состоит в большом количестве групп пользователей, из-за чего появляются сложности в управлении перекрестным доступом к информационным ресурсам.

Целю работы является: улучшение показателей доступности и конфиденциальности, при одновременном доступе пользователей к информационным ресурсам корпоративных порталов ООО «ИЦ АЙ-ТЕКО».

Предмет диссертационной работы ООО «ИЦ АЙ-ТЕКО».

Научная новизна. Предложена модель управления ИР при одновременном доступе пользователей к сети корпоративных порталов. порталов ООО «ИЦ АЙ-ТЕКО».

Данная модель базируется на следующих правилах предоставления доступа: учитывается уровень защиты данных ИР и уровня пользовательских прав.

На основе выше указанной модели информационных ресурсов, была предложена методика управления перекрестным доступом (ПД) к информационным ресурсам в сети веб-интерфейсов для доступа сотрудника к корпоративным данным.

Методика базируется на следующих принципах:

– интеграция ИР осуществляется при помощи уникального идентификатора (ID)

– передача прав доступа к ИР происходит от родительского ресурса к дочернему.

Для сети корпоративных порталов ООО «ИЦ АЙ-ТЕКО» была разработана методика организации разграничения прав при одновременном использовании ИР портала несколькими пользователями и разобраны алгоритмы её прохождения.

Разработанная архитектура автоматизированного разграничения прав при перекрестном доступе к информационным ресурсам в сети веб-интерфейсов для доступа сотрудника к корпоративным данным компании ООО «ИЦ АЙ-ТЕКО».

Диссертация состоит из следующих частей: вступительная часть, 4 главы, заключительная часть и библиография.

Глава 1 Анализ методов организации разграничения перекрёстного доступа к информационным ресурсам корпоративных поталов ООО «ИЦ АЙ-ТЕКО»

1.1 Пример практической реализации автоматизированной системы производственной деятельности предприятия

В данной главе речь пойдёт о технической деятельности компании ООО «ИЦ АЙ-ТЕКО» и практическом применении частей единой системы автоматизации.

В разработке принимает участие достаточное количество бизнес - специалистов, программистов и т.д.

В этой главе будут выделены компоненты, касающиеся только корпоративного портала ООО «ИЦ АЙ-ТЕКО».

1.2 Архитектура комплекса АСУ ООО «ИЦ АЙ-ТЕКО»

Обговаривая фактическую реализацию АСУ ООО «ИЦ АЙ-ТЕКО», нужно соблюдать созданный метод, а конкретно: предположить единое представление платформы организации, создать архитектуру, обнаружить ресурсы предоставления информативной защищенности.

Руководствоваться подобной системе необходимо вследствие того, что подобным способом, появляется максимальная возможность, сформировать лимитирования согласно доступности данных в организации, так же осуществлять представление этих орудий и приборов, при поддержки каковых сможет сформироваться концепция, форма построения нормативно-справочных сведений, далее следует осуществить представление частей комплекса.

1.2.1 Портальная архитектура АСУ ООО «ИЦ АЙ-ТЕКО»

Принимая во внимание регионально-распределительную структуру ООО «ИЦ АЙ-ТЕКО», в таком случае более результативным, отталкиваясь от архитектуры осуществления аналогичного комплекса- философия коллективного Интернет- нацеленного портала.

Коллективный портал- встроенное Интернет- дополнение класса B2E, которое предоставляет юзерам общее место допуска к информационным ресурсам.

Плюсами корпоративного портала являются:

- отсутствие в необходимости специальной подготовки персонала;

- простота в получении информации пользователем;

- сокращение цены с целью увеличения количества покупателей, посредством экономии на пользовательских лицензиях.

Постановление, основанное согласно портальному принципу, призывает конкретно к тому, что следует для результативной деятельности коллективных юзеров, а непосредственно:

- управлению моментальным допуском к данным, разнообразные методы допуска к данным, вероятность свидетельства данных в электронном варианте;

-посредственному звену – персональную рабочую зону, удобный целостный обще-пользовательский интерфейс, связь с сотрудниками;

- администраторам – интеграцию сведений так же дополнений, сквозное разделение права допуска, надзор инициативности юзеров.

1.2.2 Структура программного комплекса АСУ ООО «ИЦ АЙ-ТЕКО»

На сегодняшний день, чтобы реализовать программный комплекс с практической точки зрения, требуется осуществит выбор классической двухуровневой схемы, у которой также будет присутствовать выделенный

сервер приложений и систему управления базами данных (Oracle 10g), которая объединяет приложения при помощи бизнес-логики.

Чтобы минимизировать трафик, загрузка данных осуществляется в соответствии с *AJAX*-запросами, также осуществляется вынесение в соответствии с клиентским уровнем минимальных проверок и корректности вносимой информации, а также их реализация в соответствии с языком программирования *JavaScript* [93].

Реализация непосредственно самого портала, а также инструментов, которые позволяют управлять контентом, осуществляется в соответствии со скриптовым языком программирования *ODBiC-script*. Выполнение реализации осуществляется в соответствии и с прочими скриптовыми языками программирования без обязательных к применению функций.

Работа системы направлена на то, чтобы применять локальную вычислительную сеть рассматриваемой в текущем исследовании организации. В результате того, что применяется *Web*-доступ, работа осуществляется в соответствии со слабыми и нестабильными каналами связи. Отмечается наличие одного сервера с установкой его в администрации рассматриваемой в текущей работе организации. Система будет работать на операционной системе *Microfost Windows Server2000 Web Edition.*

«Портал характеризуется следующей структурой:

– системные и скриптовые библиотеки;

– система, позволяющая управлять контентом;

– наличие ядра портала и инструментов, для контроля доступа и разграничения прав» [33].

– система управления в соответствии с технологической нормативной справочной информацией;

– наличие специализированных дополнительных приложений на портале.

В рамках одной программной среды не представляется возможным решение всевозможных задач по автоматизации.

Например, абсолютно невозможно «расширение скриптового функционала на уровне портала с подключением дополнительных *PHP* или *ASP* модулей» [7].

Поэтому следует выбрать метод, в соответствии с которым осуществляется вызов каждой функции командной строкой, выполнение которых осуществляется в соответствии с прочими программными средами, вызов функций осуществляется через сервер, далее, клиент получает в качестве результата ответ, либо осуществляется его перенос в соответствии с кэш-директорией пользовательского сеанса. И для этого элемента характерно его применение, когда формируется клиентский отклик.

На рис.1 представлен вариант реализованных приложений и модулей корпоративного портала ООО «ИЦ АЙ-ТЕКО», где видно, как происходит разграничение доступа и затем осуществляется мониторинг режимы оборудования.

Рисунок 1 - Реализованные приложения и модули корпоративного портала

Благодаря такому методу осуществляется решение требуемых обеспечивающих задач – формируются документы в соответствии с внешними архивами, формируются графики и диаграммы посредством *Microsoft Office Web* компонента, преобразуются рисунку, кодируется код и так далее.

Также стоит отметить, что аналогично осуществляется подключение готовых PHP-библиотек, осуществляется формирование растровых карт и так далее [37].

1.2.3 Требования к пользовательским интерфейсам АСУ ООО «ИЦ АЙ-ТЕКО»

Основным правилом, для пользовательских интерфейсов, является то, что в системе должны существовать единые правила, рекомендации по построению данных.

Существует необходимость в единой библиотеке пиктограмм, единых разделов, информационных сообщений и т. д.

Необходимо использовать единую библиотеку *AJAX*-функций, доступную для юзера и позволяющую управлять содержимым информации, и кроме того выводить на экран комментарии по отображающейся информации.

«В соответствии с программным уровнем осуществляется вынесение все шаблонов по таким запросам в соответствии с отдельным контуром, в результате чего осуществляется максимально возможная унификация» [34].

Необходимо выдвигать чёткие и жёсткие требования к повышению эффективности процесса взаимодействия пользователя и ИС.

Пользовательский интерфейс – это своего рода канал связи, через который происходит взаимодействие между пользователем и компьютером.

Главными характеристиками качественного пользовательского интерфейса является возможность пользователя уделять минимальное

количество времени на изучение правил пользования интерфейсом. Интерфейс должен быть прозрачным – пользователь как бы смотрит сквозь него на свою работу. [2].

Для создания эффективного интерфейс, необходимо соблюдать следующие правила:

– интерфейс программы должен быть понятен при выполнении задачи и не усложнять её выполнение;

– выполнение задачи не должно затрудняться поиском инструкций по работе с интерфейсом;

– пользователь не должен сомневаться в корректности данных, предоставляемых программой.

Для упрощения работы с программой важно, чтобы приложения были скомбинированы в соответствии с единым стандартом.

Для упрощения работы пользователя с интерфейсом экран необходимо разбивать в соответствии с несколькими зонами, где осуществляется закрепление функциональной задачи.

На рисунке 2 представлены основные функциональные зоны корпоративного портала ООО «ИЦ АЙ-ТЕКО».

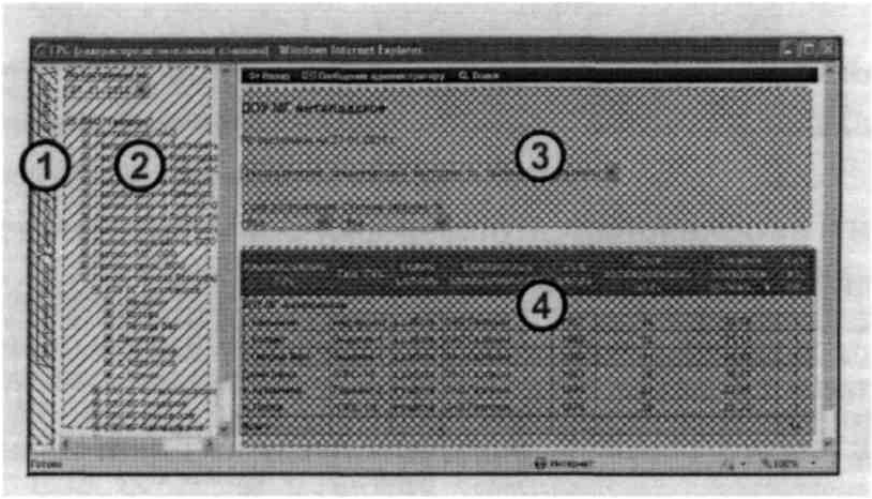


Рисунок 2 - Стандартные функциональные зоны интерфейса корпоративного портала ООО «ИЦ АЙ-ТЕКО»

Рассмотрим каждую зону:

– зона 1 выступает в качестве ориентированных по вертикали «закладок», которые требуются для того, чтобы переключать режимы, в соответствии с которыми отображается информация. Структура «закладок» определяется в соответствии с уровнем доступа;

– зона 2 выступает в качестве иерархической структуры объектов, отчеты, документы и так далее, чтобы сформировать доступ к данным в соответствии с разными правами доступа;

– зона 3 выступает в качестве заголовка страницы, сводной информации. Фильтров, инструментальных панелей;

– зона 4 выступает в качестве рабочей зоны, где отмечается наличие фундаментальных бизнес-данных в табличной форме [7].

На основании проведенного выше исследования стоит сделать вывод о том, что важными для управления эксплуатацией ООО «ИЦ АЙ-ТЕКО» являются следующие особенности восприятия:

– рабочее поле должно быть максимально заполнено полезной информацией, необходимости прокрутки экрана должны быть сведены к минимуму;

– максимальная замена пиктограммами второстепенной информации;

– на экране должна присутствовать детальная информация по задаче, взятой в работу (например, если пользователь открывает карточку подразделения, то на экране должна отображаться информация об общем количестве сотрудников и диаграммы по успешности выполнения поставленных на неделю/месяц/квартал задач) [34];

– применение легко распознаваемых пиктограмм;

– при наведении указателя на интересующий блок данных, осуществляется быстрый доступ к подробной информации.

Кроме того, следует выполнить функциональное тестирование пользовательского интерфейса на этапе проектирования системы. Тестирование должно осуществляться следующим образом:

– изучение требований к пользовательскому интерфейсу юзера;

– разработка требований и тест-планов для проверки интерфейса;

– проведение функционального тестирования и подготовка отчётов по выполненным тестам;

– выявление соответствия покрытия функциональными тестами требований;

– заведение дефектов в случае несоответствия ожидаемого результата фактическому.

Кроме того, в процессе эксплуатации всех модулей необходимо фиксировать замечания пользователей и проводить работу по улучшению качества автоматизированной системы.

1.3 Управление доступом и система разграничения привилегий в корпоративном портале ООО «ИЦ АЙ-ТЕКО»

Особое внимание необходимо уделить информации, относящейся к категории «коммерческая тайна», а также программными техническими инструментами, которые требуются для того, чтобы предотвращать несанкционированный доступ в соответствии с информацией.

Информационная безопасность сетей, с помощью которых передаются данные, в соответствии со своими глобальными вопросами и проблемами не решаются отдельно по в качестве подсистем. Если рассматривать защиту трафика, наиболее целесообразным транспортным потоком является HTTPS. Вписывание серверных ключей осуществляется посредством собственного удостоверяющего центра, а также посредством корпоративного удостоверяющего центра [36].

Ядро системы характеризуется наличием системы управления по двум фундаментальным процессам, в соответствии с которыми защищается информация – управляются пользовательские сессии и контролируется доступ в соответствии с ресурсами [7].

1.3.1 Авторизация пользователей корпоративного портала ООО «ИЦ АЙ-ТЕКО»

Процедура проверки подлинности прав субъекта осуществляется системой по его идентификатору (проще говоря, это определение имени, логина или номера).

Как правило, существуют некоторые ограничения по паролю: он не должен быть достаточно сложным, также обязательна периодическая смена пароля.

Компьютер для пользователя - вспомогательный инструмент и постоянная необходимость помнить новый пароль, затрудняет вход пользователя в систему, но тогда на помощь приходит – система аутентификации.

Аутентификация через стандартные карты доступа, является наиболее эффективной [34]. Турникеты и системы контроля доступа, на сегодняшний день, установлены во всех филиалах ООО «ИЦ АЙ-ТЕКО».

Поскольку передвижение по территории часто без карты недопустимо, для сотрудника в обязательном порядке требуется запоминать тот факт, что необходимо брать карту с собой, в результате чего операционная система компьютера блокируется, выключается экран [20].

При возвращении на рабочее место и последующем использовании карты-ключа при помощи специально установленного считывателя, автоматически становится доступным рабочий стол пользователя, при этом авторизация осуществляется по коду карты, проверяющемуся по стандартному протоколу. По причине того, что компьютер находится в защищенном помещении, вероятность физического подключения к компьютеру с целью фальсификации, значительно снижается.

Необходимо предусмотреть реализацию двух способов доступа к системе: доступ по логину и паролю (стандартный режим) и доступ по карте, в случае если рабочее место оборудовано для чтения карты.

Во время авторизации создаются пользовательские сессии. Наименование сессии осуществляется посредством произвольного символьного идентификатора, которые состоит из 20-30 букв латинского алфавита. Также стоит отметить, что, когда осуществляется авторизация, осуществляется и регистрация IP-адреса компьютера, которому предоставляется доступ. Когда осуществляются последующие запросы, адрес проверяется. Также имеется доступ к установки соответствующего пользовательского ограничения в соответствии с определенным адресом или их диапазоном. Когда сеанс завершается, осуществляется удаление кэш-директории и всех находящихся в ней файлов. Когда заканчивается рабочая смена, осуществляется принудительное завершение всех незакрытых сеансов [35]. Отсутствие активности сопровождается определенным тай-аутом, что в некоторых случаях предоставляет некоторые неудобства. Специфика работы подразумевает наличие постоянных больших перерывов между рабочими процессами. Также стоит отметить, что в результате того, что организационная структура и список абонентов телефонного справочника выстроен таким образом, что в нем отображается кадровый учет, сотрудника увольняли и доступ в соответствии с корпоративным порталом ему более не предоставлялся.

Чтобы полноценно вовлечь комплекс в соответствии с единой информационной средой компании, осуществляется выполнение интеграции в соответствии пользователями, используя централизованные управление пользовательскими правами, применяя продукт Oracle Identity Management и его аналогов [7].

1.3.2 Контроль доступа к информационным ресурсам корпоративного портала

Для упрощения администрирования корпоративного портала целесообразно использовать группировку юзеров по подразделениям,

филиалам и тому подобным, что позволяет контролировать уровни доступа пользователей внутри компании. Безопасность внутри сервера обеспечивается несколькими способами. Во первых – пароль хранится в соответствии с контрольными суммами, другими словами – если злоумышленник получит доступ к внутренней среде базы данных, он не сможет узнать пароли, чтобы войти в систему. Также стоит отметить, что каждый пользователь назначает собственный параметр доступа в соответствии с системой управления базами данных. Благодаря такому двухуровневому обеспечению защиты, осуществляется минимизация риска осуществить несанкционированный доступ, когда администратор допускает случайную, даже мелкую ошибку [20]. Контроль доступа в соответствии с приложениями осуществляется посредством того, что такой доступ настраивается, а в процессе настройки осуществляется указание уровня доступа с разной структурой шаблонов по управляющим компонентам [7].

Степень допуска для конкретной категории пользователей, может быть понижен до уровня «доступ запрещен» или напротив повышен с «базового» до «полного». При использовании подобного метода существует возможность использовать запрет на доступ к определенному подразделению, отделу и т.п. При необходимости условия «настройки» прав доступа можно организовать по зависимостям, т.е. при обнаружении переменной системой будут проверены ограничения как для текущей папке, так и для родительских.

1.4 Управление технологической нормативно-справочной информацией с использование корпоративного портала ООО «ИЦ АЙ-ТЕКО»

Задача, которая направлена на то, чтобы построить «технологическую нормативную справочную информацию под системой управления, характеризуется тем, что в нее включаются два блока:

– построение структуры информации в соответствии с системой управления базами данных» [37].

– наличие стандартных инструментов, чтобы контролировать и распределять данные [7].

«За фиксированным доменом предполагается закрепление определенной области.

При использовании транзакционных систем этот принцип нарушается, так как со временем образ предметной области меняется и это приводит к изменению структуры данных.

С применением сильно нормализованной реляционной структуры, утрачивается её простота и ясность, а изменение структуры данных вызывает сложности в поддержке РСУБД.

Целесообразно использовать общую реляционную схему, чтобы представить в ней произвольные прикладные данные, для модели которых характерна спецификация и хранение в соответствии со структурированные метаданными. Стандарт *ANSI/ISA-95.00.01-2000*, характеризуется тем, что в нем имеется описание рекомендаций, которые направлены на то, чтобы осуществлять такую модель, что изначально было базой. Тем не менее, для стандарта *ISA-95* не характерно предоставлять конкретные рекомендации [7].

В результате этого для каждого объекта предметной области предусматривается их группировки в соответствии с достаточно стабильными и свободными системами – классами, где формируются наименование параметров – атрибутов [3].

Формирование класса, другими словами – потомка, осуществляется в соответствии с созданным родительским классом, когда для потомка характерно наследование атрибутов родительского класса. Описание связей в соответствии с каждым объектом предметной области осуществляется посредством отношений классов по ассоциациям, композициям.

Если реализовать систему в соответствии со стандартом *ISA-95*, сформировать на его основе метаданные, осуществляется формирование

достаточно сложных логических структур, чтобы описать модель в соответствии с предметным направлением, структура которой характеризуется большим разнообразием объектом, где формализуются ограничения и целостность информации» [7].

«Плюсом этого подхода в структуре удобство не только паспортной информации, но и бизнес-информации [36]»

При всем этом, можно смело утверждать, что затраты труда полностью отсутствуют, а управление структурой данных на высоком уровне приспосабливаемости привело к возможности стремительного развития специализированных дополнений «от малого к большому»

1.5 Средства управления контентом и администрирования корпоративного портала ООО «ИЦ АЙ-ТЕКО»

Спецификой ИС, созданных для автоматизации деятельности является факт, что администрирование бизнес-логикой, отчётность и остальными немаловажные задачи необходимо доверять только лицам, которые максимально соприкасаются с бизнесом.

Наиболее качественно данную работу выполнят внутренние сотрудники, знающие специфику работы компании ООО «ИЦ АЙ-ТЕКО», а не привлечённые специалисты.

Поэтому данная система в обязательном порядке должна содержать среду управления и разработки, для того чтобы эффективно использовать, разрабатывать и отлаживать приложение даже человеку, не имеющему специальных знаний, умений и навыков программиста.

Необходимо разработать простую в управлении, но в то же время эффективную среду управления экранными формами - *«Web-портал конструктор»,* для обеспечения качественного выполнения поставленных задач.

Необходимо иметь возможность создавать остальные приложения только с использованием данного конструктора, в том числе это относится к средствам администрирования.

1.6 Анализ существующих систем управления доступом к информационным ресурсам

В соответствии с текущей главой осуществляется рассмотрение программных технических инструментов, чтобы обеспечить доступ и контролировать его в соответствии с ИР корпоративными сетями.

Безопасность обеспечивается посредством многофункционального инструмента Cisco Adaptive Security Appliance.

Позволяет получать полное представление о сетевой инфраструктуре, повышает уровень информационной безопасности, путем мгновенного предотвращения известных и неизвестных атак, а также обеспечивает единую платформу управления с возможностью выполнять конфигурацию средств защиты.

Для каждого устройства характерно выступать в качестве маршрутизатора доступа. Благодаря установленному в соответствии с границей сети шлюза, осуществляется формирование доступа к сети Интернет. Защита доступа обеспечивается посредством удаленных пользователей подразделений, межсетевым экраном, функциями, которые идентифицируют и авторизуют пользователей, а также осуществляется разграничение пользовательского доступа в соответствии с внутренними ресурсами сети с получение пользовательской статистики [7].

Мультисервисный шлюз управления (MSCG) Huawei Quidway Broadband AccessServer, предназначен для управления IP-сетью, предоставляя доступ к сети Интернет, услугам связи, голосовым и видео услугам, 3g и NGN, обеспечивая разделение пользовательских данных и данных управления, иерархическую авторизацию пользователей, управление

перегрузками. Надежная защита от несанкционированного доступа и действий злоумышленников обеспечивается механизмом отторжения атак DoS, шифрованием данных, а также использованием высокоэффективного брандмауэра с непрерывным мониторингом и журналированием состояния соединений.

Для прокси-сервера характерна защита сети от внешних угроз. При этом прокси-сервер контролирует интернет трафик Microsoft ISA Server (Active Directory).

Благодаря ему локальная сеть защищена в соответствии с посторонними вмешательствами сети Интернет и безопасной публикацией разнообразных категорией серверов с предоставлением возможности распределение пользовательского доступа к разнообразным Интернет-ресурсам. Прокси-сервер характеризуется наличием инструментов, чтобы проанализировать посещаемые ресурсы, учитывать трафик, а также защищать сеть от внешних угроз. Также стоит отметить, что для прокси-сервера характерно наличие разнообразных методов аутентификации и авторизации, осуществляется поддержка рабочей группы и домена Windows NT. Также характерно наличие большого количества плагинов, чтобы отследить исходящий и входящий трафик.

В ходе анализа представленных решений можно сделать вывод, что ориентация приложений идёт в соответствии с применяемыми внутрисетевыми технологиями, где отмечается корпоративный доступ. Также стоит отметить наличие трудностей в том, чтобы интегрировать в соответствии с единой информационной сетью, так как это может являться причиной тому, что разнообразные приложения попросту будут несовместимы. Таблица 1 представлена в соответствии с тем, что сравнивается система аналогов.

Таблица 1 - Сравнение систем-аналогов

Наименование показателя	Cisco ASA Server	Nortel Contivity Secure IP Services Gateways	Huawei Quidway Broadband Access Server	Microsoft ISA Server (Active Directory)
Поддерживается безопасная аутентификация, пользовательская авторизация – управляются учетные пользовательские записи	+	+	+	+
Имеются инструменты для того, чтобы формировать и управлять доменными категориями	-	-	-	+
Возможно устанавливать доверительные отношения в соответствии с доменными категориями	-	-	-	+
Наличие Web-интерфейса аутентификации и управления	+/-	+/-	+/-	+/-
Поддерживается фильтрация структурных составляющих протокола HTTP	+	+	+	+
Поддерживается безопасный доступ в соответствии с протоколом HTTPS	-	-	-	+
Поддерживается технология VPN	+	+	+	+
Разграничивается доступ в соответствии с разделами порталов в соответствии с пользовательскими правами	+/-	+/-	+/-	+
Работают внешние сервера аутентификации и управляются учетные записи	+	+	+	+
Имеются инструменты в соответствии с Web-интерфейсом				+/-
Имеются инструменты Web-интерфейса, чтобы формировать, управлять и контролировать мета информационное описание структура портала	-	-	-	+/-
Возможность использования решений для того, чтобы работать с публичными каналами глобальной сети	+	+	+	+/-
Портал функционирует в соответствии с разнообразными платформами	+	+	+	-
Функционирование системы в соответствии с разнообразными аппаратными платформами	-	-	-	+
Система функционирует в соответствии с доступной программной платформой	-	-	-	-
Имеются инструменты, которые позволяют учитывать пользовательские реакции и действия	+	+	+	+

В соответствии со сравнением системы аналогов осуществляется формирование следующих выводов:

Взаимодействие системы управления доступов в соответствии с ресурсами осуществляется по рынку завершенными аппаратными решениями, когда рассматривается узкая специализация, а также многофункциональны программные инструменты [3].

Предоставление доступов к ИР является актуальной темой на данный момент. Вместе с тем, интеграция нескольких порталов в единый корпоративный портал связано со многими сложностями. Требуются дополнительные затраты на лицензирование использования программного обеспечения. Необходимо наличие отдельного *Web*-сервера для первых трёх производителей, а также применять дополнительные инструменты внедрения. Для таких производителей не характерно наличие гибких инструментов, которые позволяют управлять и контролировать доменные категории и групповые политики.

Для программного решения Microsoft характерно наличие инструментов, которые позволяют управлять и контролировать групповые и доменные категории, тем не менее – осуществляется формирование жестких ограничений в соответствии с функционированием платформы, что выступает в качестве неприемлемого, если рассматривать тот факт, что портал рассчитан на автономное функционирование. Для такого программного решения не характерна адаптация в соответствии с тем, чтоб работать посредством каналов глобальной сети [3].

1.7 Требования к системам в области управления перекрёстным доступом к информационным ресурсам корпоративных порталов ООО «ИЦ АЙ-ТЕКО»

На концепции мониторинга положения изучений в сфере и теории изложенной в структуре разделения допуска с задачей выстраивания

распределённой сетки клиентских серверов, были выдвинуты следующие тезисы:

Благодаря программно-аппаратной площадке возможна эффективная разработка механизмов разделения допуска к информационным ресурсам в сети клиентских серверов ООО «ИЦ АЙ-ТЕКО», с предоставлением качественной защиты информации от незаконного допуска (НСД).

Особенность информационного обмена в корпоративных порталах через открытые каналы коммуникации Интернет в рамках клиентских серверов ООО «ИЦ АЙ-ТЕКО» через Web-сервера заключается во взаимодействии с разнородными, распределёнными, осуществлёнными на предпосылке различных технических решений объемами данных.

Унификация аппаратно-программных площадок развития серверов, формулы понятия, хранения информации и схемы допуска к ней в разнообразнейших корпорациях рассматривается как энергозатратный и недешевый вариант урегулирования трудностей.

При помощи формирования программного механизма администрирования взаимодействия пользователей возможно достичь уменьшение цены построения клиентских серверов и снижения трудоёмкости.

«В каждом из методов на этапе обоснования спецификаций возводятся модели, характеризующиеся»[3] прямым восприятием действительных предметов и механизмов объектной сферы.

Выводы к главе 1

Характерной чертой деятельности ООО «ИЦ АЙ-ТЕКО» является следующие способы интеграции:

– вертикальная интеграция, которая представляет собой передачу данных снизу вверх по схеме и ликвидацию различий в справочной информации.

– горизонтальная интеграция позволяет разным задачам, а также юзерам использовать всю свою (и разрешенную в строгом соответствии с политикой разделения доступа) информацию, вычислительные массивности, программы.

Средства администрирования и управления контентом корпоративного портала, ориентированы на исполненье стандартных функций управления ИС корпоративного уровня, отличающихся от информационно-аналитических систем, созданных для автоматизации производственной инициативности, поскольку дают обеспечение управление бизнес-логикой и имеют в личном составе визуальную среду разработки, которая дает возможность использовать дополнения, без особых знаний, навыков и умений программиста.

При авторизации пользователя фиксируется IP-адрес компьютера, с которого был осуществлен вход. Затем, при последующих запросах или авторизации в системе проходит проверка этого IP-адреса.

Поставленную задачу необходимо решать основываться на разработке сети веб-интерфейсов для доступа сотрудников к корпоративным данным, в которой происходит интеграция ИР организации ООО «ИЦ АЙ-ТЕКО».

Разработанная система должна быть центром управления, классифицирующим ИР, управляющим перекрёстным доступом в рамках сети.

Кроме того, через закрытые разделы корпоративных порталов должна существовать возможность и контролировать информационное взаимодействие в соответствии с центральными системами управления сети, а также корпоративной системы управления организаций.

Глава 2 Разработка формализованной модели управления перекрестным доступом к информационным ресурсам в сети корпоративных порталов ООО «ИЦ АЙ-ТЕКО»

2.1. Анализ существующих подходов к моделированию управления доступом

Если мы обратим внимание и совершим разбор по дискреционной модели, мандатной и ролевой, другими словами, по традиционным моделям управления доступом к ИР, то увидим, что традиционные модели, исполнены благодаря модели управления перекрёстным доступом к информационным ресурсам сети корпоративных порталов, которые приспособлены к условиям функционирования и практическим нюансам реализации современных корпоративных порталов ООО «ИЦ АЙ-ТЕКО»[1].

Следует ознакомиться и проанализировать традиционные модели управления доступом к ИР, точнее: дискреционную модель, мандатную и ролевую модели.

Традиционные модели, будут выполнены при помощи модели управления перекрёстным доступом к ИР сети корпоративных порталов, приспособленными к условиям функционирования и практическим нюансам реализации современных корпоративных порталов ООО ИЦ АЙ-ТЕКО [1].

2.1.1 Модели дискреционного управления доступом

Есть конкретные требования, которым соответствует дискреционная модель управления:[22].

– для каждой сущности в обязательном порядке характерно наличие уникального идентификатора;

– соответствие любой строки субъекту матрицы доступа, для столбца характерно наличие любого подхода в соответствии с сущностью, в ячейке

имеются правовые разрешения доступа субъекта в соответствии с сущностью, что выступает в качестве большого разнообразия в соответствии с реализованными правами доступа; [7].

– в такой ситуации, когда ячейка имеет соответствие субъекту и сущности, отмечается наличие определенного обладания прав доступом.

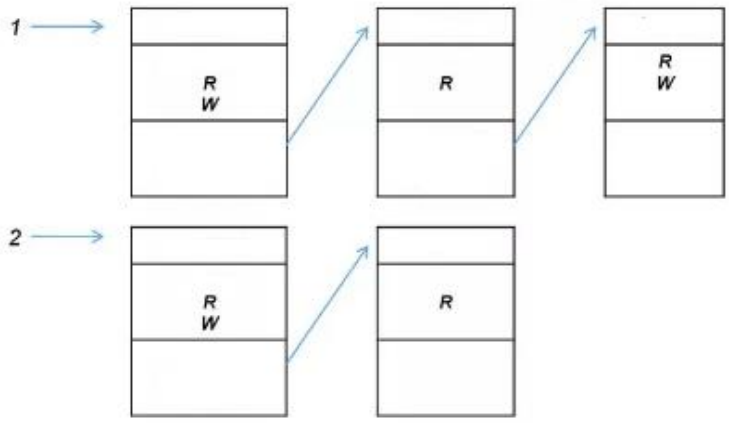


Рисунок 3 - Дискреционная модель доступа к ИР

На рисунке 3 схематично представлена дискреционная модель доступа к ИР, где R означает чтение, W – запись.

Но необходимо отметить, что наиболее известными образцами дискреционных моделей управления доступом считают:

– Модель Take-Grant

– Модель Харрисона-Руззо-Ульмана [14, 22].

Простота реализации модели является ярко выраженным преимуществом дискреционной модели управления доступом.

Учитывая этот факт, в сегодняшней современности, большое количество систем управления доступом используют конкретно эту модель [1, 32]

Есть и определённые изъяны модели дискреционного управления доступом: присутствие статичности правил управления доступом.

2.1.2 Модели мандатного управления доступом

Конкретные и немаловажные требования имеются и по отношению к Мандатной модели управления [14]:

– осуществляется формирование решетки в соответствии с уровнем конфиденциальности;

– любая сущность характеризуется собственным индивидуальным уровнем, в соответствии с которым осуществляется формирование соответствующих ограничений по доступу к сущности;

– для любой сущности предусматривается ее идентификация;

– каждый субъект обладает в обязательном порядке привилегиями, в соответствии с которым осуществляется формирование уровня обязанности;

– для реализованной сущности не характерно иметь новые потоки данных от сущностей, которые имеют повышенный конфиденциальный статус в соответствии с сущностями, у которых заниженная конфиденциальность.

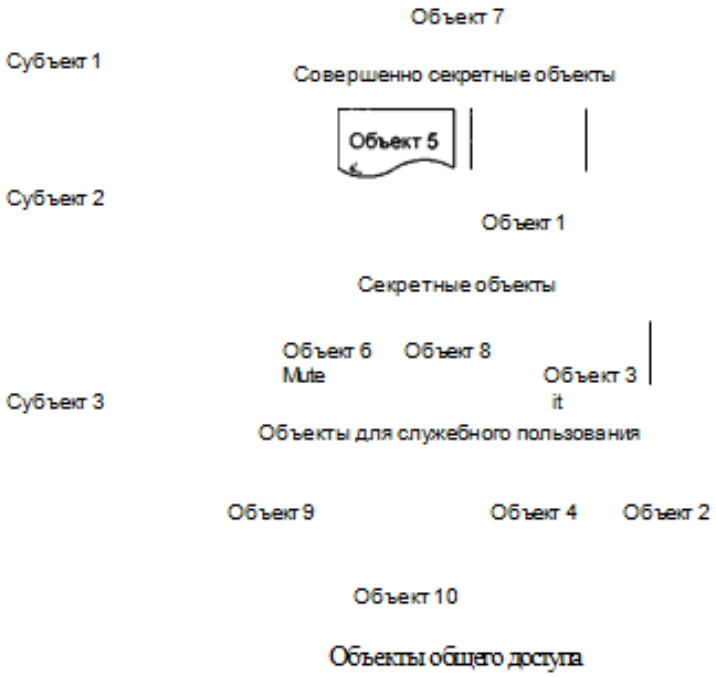


Рисунок 4 - Мандатная модель доступа к ИР

Рисунок 4 наглядно демонстрирует мандатную модель доступности к ИР.

Наиболее приемлемым примером мандатной модели управления доступом можно обозначить модель Белла-Лападулы. Требования мандатной модели управления доступом более прозрачны для разработчиков и юзеров, это может послужить дополнительным нюансом повышенного уровня надёжности этой модели [4, 32].

Но, реализация данной модели управления достаточно сложна принуждает к использованию источников вычисления.

2.1.3 Модели ролевого управления доступом

Необходимо чтобы ролевая модель управления доступом имела соответствие последующим требованиям: [14].

– Идентифицированность сущностей;

– Большое количество ролей, имеющих аналогичное количество прав доступа к сущностям;

– Любой из субъектов обязан владеть некоторым количеством разрешенных ролей для данного субъекта;

– Только в случае, когда субъект обладает правом доступа к сущности он допускается к этой сущности.

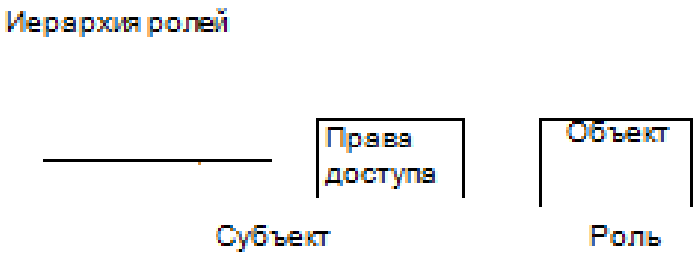


Рисунок 5 - Ролевая модель доступа к ИР

Рисунок 5 наглядно демонстрирует ролевую модель доступа к ИР.

То, откуда начинается политическое развитие дискреционного управления доступом, можно назвать, ролевым управлением доступом, не смотря на всё это, правообладание доступом субъектов системы к сущностям кооперируются благодаря особенностям их специфичного применения, за счёт которого образуются роли. [4].

Благодаря заданию ролей более точными и прозрачными становятся требования к управлению доступом.

2.2 Формализованная модель управления перекрёстным доступом к информационным ресурсам в сети корпоративных порталов ООО «ИЦ АЙ-ТЕКО»

Для будущего изучения преимуществ и недостатков необходимо сделать акцент на процессе управления перекрёстного доступа к ИР в сети корпоративных порталов ООО «ИЦ АЙ-ТЕКО».

Стоит отметить наличие следующих положений в соответствии с классическими моделями того, как разделяется доступ в соответствии с компьютерными системами:

«- Дискреционное;

– Мандатное;

– Ролевое» [35].

Требуется формирование модели управления, у которой будет перекрестный доступ в соответствии с информационными ресурсами в сети по корпоративным порталам рассматриваемой в текущей работе организации.

Ее формальное представление выглядит так:

$$M = \{U, D, P, R, S, Z, W, F), (1)$$

«U = {ui,u2,... $u_{ис}$ } - множество субъектов доступа (пользователей), при $_{ис}$ - количестве субъектов доступа.

В пределах протоколов, получивших разрешение (HTTP/HTTPS) субъекты множества производят обмен информацией.

Рисунок 6 - Процесс управления перекрёстным доступом к ИР

Любому субъекту аналогичен набор уникальных (в рамках пользовательского домена) идентификаторов (ID)

$I = \{i_1, i_2, \ldots, i_{ic}\}$- множество ID, при $_{ic}$ - количестве ID.

Для однозначного распознавания субъектов среди суммарного количества элементов множества U служат ID.

При помощи аутентификаторов из множества A можно уверенно утверждать, что субъект конкретно тот, кем себя представляет, таким образом,

$A = \{a_1, a_2, \ldots, a_{ac}\}$ — множество аутентификаторов, при $_{ac}$ — количестве аутентификаторов»[22].

Формирование элемента в соответствии с рассматриваемым множеством осуществляется в соответствии с тем, когда субъект впервые обращается к объекту за идентификацией и аутентификацией.

Также стоит отметить сохранение идентификатора и аутентификатора в соответствии с сессией – повторный ввод не нужен, когда пользователь обращается к определенному ресурсу.

Есть некоторые функции:

sid: S —>I, *suser*:

S —>U, *sauth*:

S —>A.

Они присоединяются к множеству базовых функций системы - F, т. е.

{*suser, sid*} C F.

W = {w_1,w_2,…w_{wc}) - множество Web-порталов, при wc - количестве Web-порталов.

Не стоит забывать о том, что отмечается наличие возможности внесения дополнительных ограничений, чтобы достичь высокий уровень гибкости управления, к примеру:

- В какой продолжительности осуществляется сессия пользователя,

- Как соединены компоненты и так далее.

Изучение модели указало, что для решения поставленных задач, введенных в модель системы компонентов, вполне достаточно.

2.3 Модель доменов пользователей

Есть основополагающие и важные причины для создания продуктивного метода управления перекрёстным доступом в сети корпоративных порталов ООО «ИЦ АЙТЕКО»:

– чёткое описание целой структуры предмета управлений:

– конкретных связей частей концепции, структуры информативных источников, а так же, требований взаимодействия;

– функционирования компонентов концепции.

Форму информативного взаимодействия комфортнее всего изучать в виде иерархической концепции модификаций.

На начальном уровне изучается связь юзера с системой в аспекте предоставления ему конкретного комплекта услуг.

Модели наиболее высочайшей степени представляют элементы протекания того или другого хода в рамках определённого процесса базисной модели и, так же, имеют все шансы включать в себя:

– организационные нюансы взаимодействия;

– технические нюансы взаимодействия;

– организационно-технические нюансы взаимодействия.

Юзером концепции обычно является конкретный индивид либо технический прибор, который посылает запросы концепции посредством телекоммуникационных каналов взаимосвязи и приобретает от нее результат в варианте предоставления допуска к конкретному ресурсу или отказа в нем.

В рамках концепции принято считать, что пользователь- это член одной (без исключения) компании, входящей в структуру сети порталов.

Для наружных юзеров, которые не причастны ни к одной из данных компаний, вводится вспомогательная вымышленная организация. Членом этой вымышленной компании принято считать любого юзера, который не имеет регистрации в системе, при всём этом, любые юзеры имеют равные права и низкоуровневый доступ.

Большое количество пользователей, у которых есть регистрация в системе в качестве участников одной из поддерживаемых компаний, создают домен юзеров.

Для доменов характерно их разделение в соответствии с поддоменами, в результате чего осуществляется формирование иерархии.

Значимым фактором считается недоступность этой иерархии, другими словами, разделение домена имеется только лишь в рамках существующего домена и заметна лишь участникам этого домена, с точки зрения других элементов концепции домен представляет собой единое целое [3].

Индивидуальный уровень доступа должен иметь каждый пользователь.

Для уровня допуска характерно выступать в качестве целочисленного показателя, в соответствии с которым указывается ресурс в соответствии с доменом пользователя доступа [3].

Формирование доступа у пользователя в соответствии с источником появляется тогда, когда для источника характерно его отнесение в соответствии с доменом пользователя. Также стоит отметить, что для допуска характерно приравниваться или быть меньше уровня, если приводить в сравнение приватность ресурса.

Другими словами, пользователь *u* имеет доступ к источнику *res,* в

случае:

$$3\{domain, privacy) \in Dr\{res) : domain \in Dp(u)\&privacy > access(u), (2)$$

Где:

D_r - оператор получения множества пар, характеризующих ресурс (характеристического множества);

D_p - оператор получения множество доменов (иерархии доменов), в которых состоит пользователь;

access - функция уровня допуска пользователя.

В этой постановке задачи актуально сопоставление уровней доступа в различных доменах первого уровня [3].

Отсутствие согласованности приводит к некорректному назначению уровня доступа.

Это приводит к тому, что некоторые пользователи получают завышенный уровень доступа, который не был согласован.

Из чего следует, что для большей гибкости в совместном использовании информационных ресурсов, необходимо использовать иерархию доменов.

Рассмотрим, к примеру, доступ к ИР подразделения

При составлении домена пользователей сотрудники компании имеют возможность получить доступ к определенным ИР подразделения, при этом существует возможность разграничения доступов внутри подразделения.

Для работы каждого отдела подразделения может требоваться доступ к конкретным ИР и недопустим доступ к другим ресурсам.

Для получения уникальных доступов сотрудников отделов используется разделение, путём добавления следующих пар: домен подразделения, приоритет и домен департамента, приоритет.

Уровень доступа и привилегий, необходимые для просмотра информации, определяются установлением уровня конфиденциальности.

В некоторых случаях доступы сотрудников одного отдела необходимо иметь коллегам из других отделов, как правило это управляющие.

В качестве решения данной ситуации используется добавление пар к параметрам данных определенных ресурсов, основным элементов будет домен конкретного отдела.

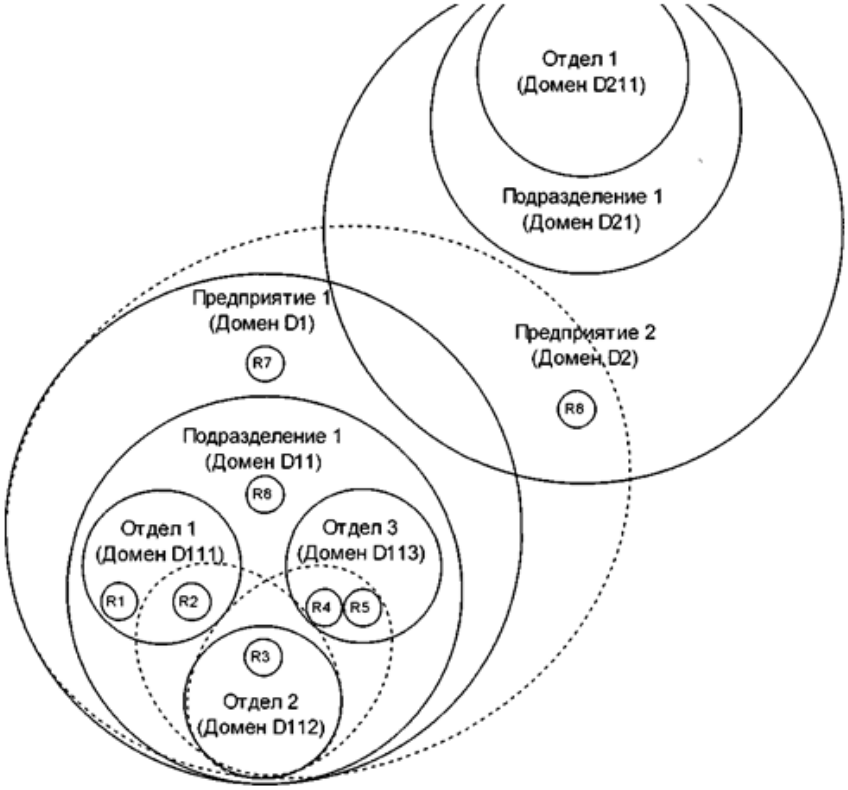


Рисунок 7 - Пример разделения ресурсов и иерархии доменов

Рисунок 7 демонстрирует схему распределения ресурсов и иерархии доменов.

Где:R_i –предоставляемые доменом ИР (домены представлены в виде окружностей)

D_i - название домена.

Пользователи определенного дочернего домена обладают доступом к

любым источникам доменов, стоящих на порядок выше (само собой предполагается, если уровень допуска имеет высокий уровень).

Помимо этого, юзеры домена *D112* применяют доступность к определённым источникам доменов, расположенных по соседству.

Рисунок 7 продемонстрировал домен другой компании, в пределах которой находится ресурс *R8*.

Этот источник доступен юзерам домена *D1*, при всем при том доступ к источникам закрыт для пользователей домена *D2*.

Большое количество характеристик, которые на рисунке 2.5 информационных источников имеют следующий вид (уровень приватности любого ресурса приравнивается нулю):

$$Dr\ (R1)\ =\ \{(D111,0)\}$$
$$Dr(R2)\ =\ \{(D111,0),(D112,0)\}$$
$$Dr(R3)\ =\ \{(D112,0)\}$$
$$Dr(\ R4)\ =\ \{(D112,0),(D113,0)\}$$
$$Dr(\ R5)\ =\ \{(D112,0),(D113,0)\}$$
$$Dr(R6)\ =\ \{(D111,0)\}$$
$$Dr(R7)\ =\ \{\{DU1,0)\}$$
$$Dr(R8)\ =\ \{(Dl,0),(D2,0)\}$$

Например, юзеры всех доменов *Dlln,n* = 1n где п – количество поддоменов домена *D11*,есть возможность получить доступ к источникам *R6*. Так, аналогичная система предоставляет высокий уровень приспосабливаемости в управлении предоставлением доступов к ИР.

Также требуется проанализировать применение уровней доступа пользователей в граничных значениях поддоменов.

Необходимо прописать правила, которые будут распространяться на каждый домен, не исключая домены по умолчанию, не принадлежащие конкретной организации.

Для удобства использования, можно применить следующую шкалу уровня доступа к ИР: от 0 до 20, где ноль будет соответствовать гостю, без особых полномочий, а 20 – системному администратору, который имеет полный доступ ко всем ИР.

При таком подходе остается не охваченной задача предоставления юзерам информации о существовании ресурсов, к которым они не имеют доступа.

Не всегда является корректным не предоставлять юзерам информацию, которая не соответствует уровню привилегии данного сотрудника.

Можно представить факт существования каталога IRS предприятия, к которому внешний юзер не имеет доступа, потому, как эти источники считаются интеллектуальной собственностью этой компании.

Несмотря на это, компания без затруднения в силе предложить данные материалы, чтобы в последующем использовать их в коммерческих целях.

Исходя из этого становится ясно, что пользователям, зачастую, необходимо владеть информацией о существовании закрытых источников и иметь возможность запросить этот доступ.

Чтобы решить рассматриваемую проблему, требуется применение системы показателей в соответствии с источниками.

В соответствии с рассматриваемой системой осуществляется присваивание определенного показателя для каждого источника, в соответствии с которым осуществляется определения уровня его конфиденциальности в соответствии с поиском, публикацией и так далее.

Можно выделить три уровня доступа: «Открытый», «Закрытый», «Ограниченный». При наличии уровня доступа «Открытый» - доступ возможен как для сотрудников, так и для гостей. Уровень доступа «Закрытый» предполагает, что доступ имеет узкий круг сотрудников, которым данный доступ был предоставлен. В случае если доступ «Ограниченный» - доступ получают сотрудники, которые обладают

необходимым уровнем доступа соответствующему их грейду или более высоким уровнем.

Необходимо обратить внимание, что данная система будет работать корректно только в том случае, если система назначения уровня допуска согласована в различных доменах.

Установление индивидуального уровня доступа для каждого пользователя домена занимает большое количество времени, т.к. системой пользуется большое количество юзеров.

При этом необходимо учитывать, что существуют ситуации, когда индивидуальный доступ необходим, поскольку пользователь помимо принадлежности к домену должен обладать правами предназначенными для какой-либо социальной или профессиональной группы.

Пользователи определенной группы обладают похожими социальными или профессиональными потребностями и равноценными правами.

В том случае, когда сотрудник состоит в нескольких таких группах, то в каждой отдельной группе он имеет полный доступ.

Именно так отличается домен, где применение доступа осуществляется в соответствии с иерархией без учета подразделения, где оформляется работник.

Такой момент важно учитывать для того, чтобы стереотипно присвоить права доступа, так как осуществляется определение качественных групп пользователей, разделение их в соответствии с сотрудниками, менеджерами, высшим руководством, когда не учитывается то, как они распределяются в соответствии с подразделениями предприятия[3].

Выводы к главе 2

Данная глава была составлена для анализа традиционных моделей управления доступом в соответствии с дискреционной модель, мандатной и ролевой моделью, что и было выполнено в текущей главе диссертационной

работы.

Также осуществляется разработка и предложение модели управления доступом в соответствии с корпоративными порталами.

Приняты за фундамент правила доступа к информационным ресурсам.

Было установлено, уровень привилегий, представленный в виде индикатора и определяющий к каким ИР юзер имеет доступ в рамках домена.

Уровень привилегий определяется уровнем конфиденциальности, присвоенной пользователю.

Выявлено, что существует возможность вносить дополнительные ограничения для достижения высокого уровня гибкости управления, например:

- продолжительность сеанса пользователя,

- тип соединения между компонентами и др.

Была предложена система доменов, существующих в иерархии, пользователей и использование групп, внутри которых пользователи обладают равноценными правами.

Кроме того, было предложено использовать систему индикаторов для ресурсов, определяющих возможность осуществить какие-либо операции.

Было выявлено, что существует возможность не учитывая подразделения, к которым принадлежит пользователь, объединить пользователей по уровню.

Таким образом возможно предоставление прав пользователям исходя из критериев занимаемой должности в организации.

Глава 3 Разработка методики управления перекрёстным доступом к информационным ресурсам в сети корпоративных порталов ООО «ИЦ АЙ-ТЕКО»

3.1 Особенности анализа функциональных требований к системе

Требования, которые осуществляют применение формализованной модели, создаются и анализируются в качестве основополагающей стадии, когда применяется модель в соответствии с программными системами.

Цель: полностью проверить требования с их приоритетами, осуществить изучение функциональности и граничных значений системы с анализом взаимосвязи архитектуры ПО и модели.

Когда разрабатываются программные системы в соответствии с технологией UML [7], работа которой связана в соответствии с тем что применяется программная система, чтобы сформировать определенную модель.

В модели вариантов, действующие лица - это пользователи системы.

Варианты использования – это действия, которые выполняют действующие лица.

Пользователь видит каждый случай, как череду событий в программной системе [5].

Следующие функции выполняют примеры использования в программных системах:

– каждый пример имеет соответствующие функциональные требования в соответствии с программной системой.

– определение системы в соответствии с прецендентами осуществляется посредством модели методов применения [3].

Для вариантов применения характерно структурирование каждой объектной модели.

Для предотвращения препятствий в работе с действительной программной системой, требуется осуществить структурирование ее объектных моделей, классов так, когда для каждой из них характерно выступать в качестве конкретного фактора ее применения.

В этой ситуации для каждого аспекта предусматривается его соответствие прецедентам, когда в его описании отмечается наличие лишь тех объектов, для которых характерно выступать в качестве участника в соответствии с такими прецедентами [3].

В соответствии с разнообразными вариантами использования, осуществляется применение одного и того же объекта.

3.2 Концептуальный подход к управлению доступом в сети корпоративных порталов предприятий

Осуществляется формулировка фундаментальных функциональных задач, а также определение специфика работы.

В соответствии с тем, что была проанализирована внешняя информационная среда, осуществляется выявление действительных пользователей системы с определением их функциональных потребностей.

В соответствии с тем, что были проанализированы требования и внешняя среда, требуется выявление функционального значения пользователей системы управления, а также функциональных требований системы.

Выявлены следующие основные пользователи системы управления по следующим категориям:

- наличие неавторизированных пользователей, которые получают доступ в соответствии с ограниченным количеством разделов портала, на котором не отмечается необходимость в особом доступе;

– для авторизированных пользователей характерно выступать в качестве таких пользователей, в соответствии с право обладанием которых

осуществляется получение доступа в соответствии с закрытыми разделами портала. Каждый пользователь характеризуется наличием единственной группы прав доступа.

– для администраторов доступа характерно выступать в качестве таких пользователей, в соответствии с которыми осуществляется формирование уровня привилегий, чтобы другой пользователь получил доступ в соответствии с закрытыми разделами портала. Также они осуществляют определение разделов для открытия и закрытия.

Далее, следует проанализировать функциональные требования п спецификации в соответствии с системой контроля информационного обмена, что в текущей работе было целесообразно представить в табличной форме в таблице 2.

Таблица 2 – Спецификация функциональных требований в системе

Обозначение	Наименование требования
1	Управление сетью порталов
1.1	Создание и удаление пользовательских доменов
1.1.1	Создание и удаление групп уровней доступа
1.2	Связывание доменных групп с порталами
1.3	Делегирование полномочий администрирования доменов
1.4	Мониторинг обновления информации о пользователях
1.5	Мониторинг модификации данных о структуре порталов
1.6	Репликация данных о структуре порталов и правах доступа
1.7	Репликация данных о пользователях и группах
1.8	Разрешение доступа доменным группам к другим порталам
2	Управление доступом к порталу
2.1	Мониторинг доступа к порталу
2.2	Формирование и модификация структуры каталогов портала
2.3	Назначение ограничений доступа к разделам
2.4	Назначение уровней доступа к закрытым разделам портала
3	Управление пользователями домена
3.1	Мониторинг активности пользователей
3.2	Модификация учетных записей
3.3	Создание и удаление учетных записей пользователей
3.4	Изменения членства пользователей в группах доступа
4	Мониторинг функционирования комплекса в целом
5	Резервное копирование данных
6	Мониторинг функционирования системы доступа
7	Доступ к закрытым разделам портала

Продолжение таблицы 2

7.1	Поиск информации в открытых разделах
8	Доступ к открытым разделам портала
8.1	Перехват и анализ трафика
8.1.1	Проверка статуса ресурса
8.1.2	Аутентификация пользователя
8.1.2.1	Переадресация аутентификации на сервер сети
8.1.3	Подтверждение полномочий
8.1.3.1	Переадресация авторизации на сервер сети
8.1.4	Перенаправление трафика на web-сервер портала
8.2	Поиск информации в закрытых разделах

Расположение требований осуществляется на основании указанных выше категорий.

3.3 Построение прецедентной модели системы

Осуществляется формирование модели того, как применяется система в соответствии с тем, что были проанализированы требования и внешняя среда систему управления обменом информации, когда применяются поддерживающие инструменты в соответствии с технологией UML.

Рисунок 8 составлен для более удобного схематического представления того, каким образом для администраторов будет характерно применение системы относительной того, какие функциональные возможности доступны для администраторов.

Рисунок 9 составлен для более удобного схематического представления того, как применяю систему пользователя в соответствии с тем, чтобы использовать информационные ресурсы портала.

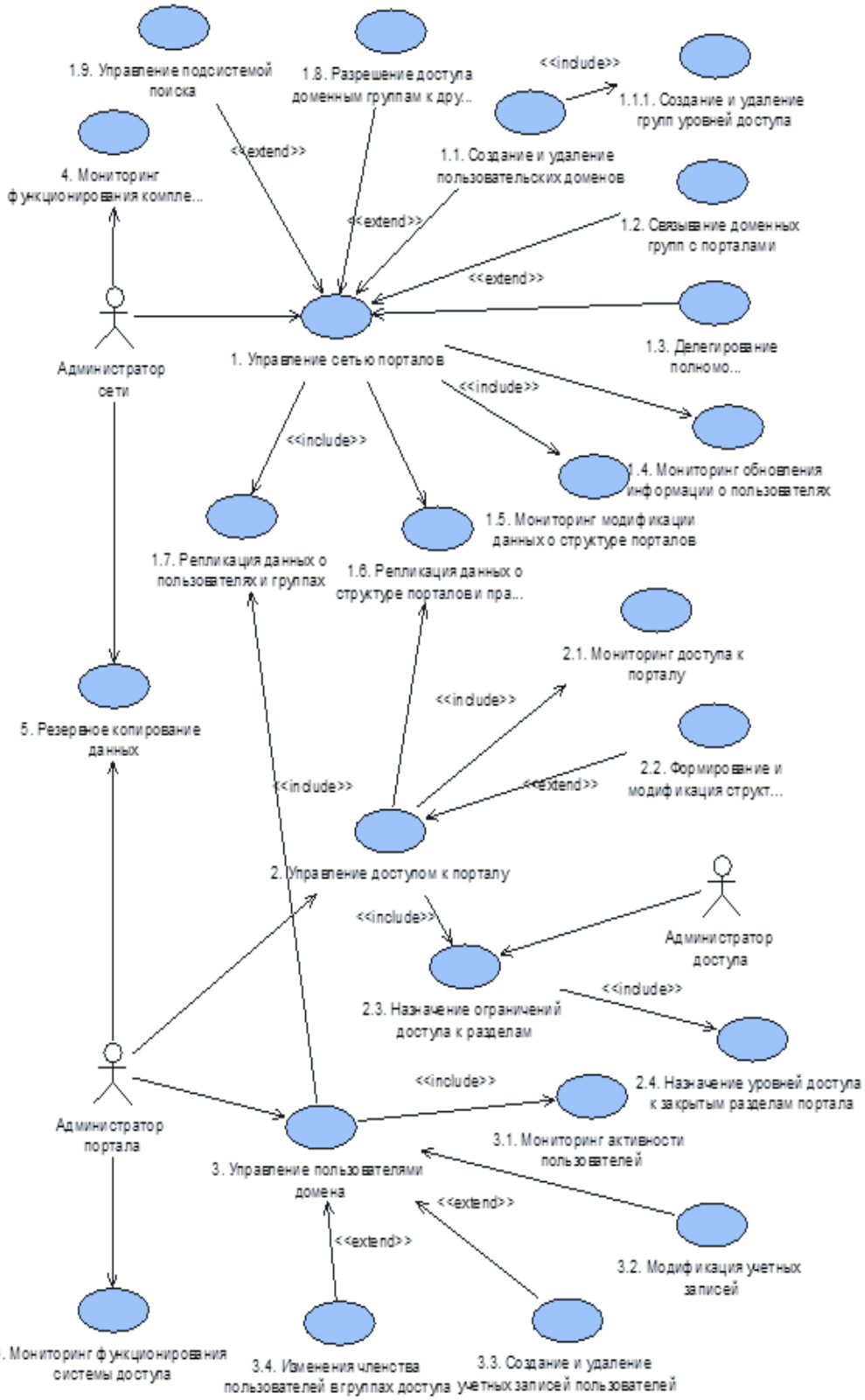


Рисунок 8 - Прецедентная модель функций управления системы

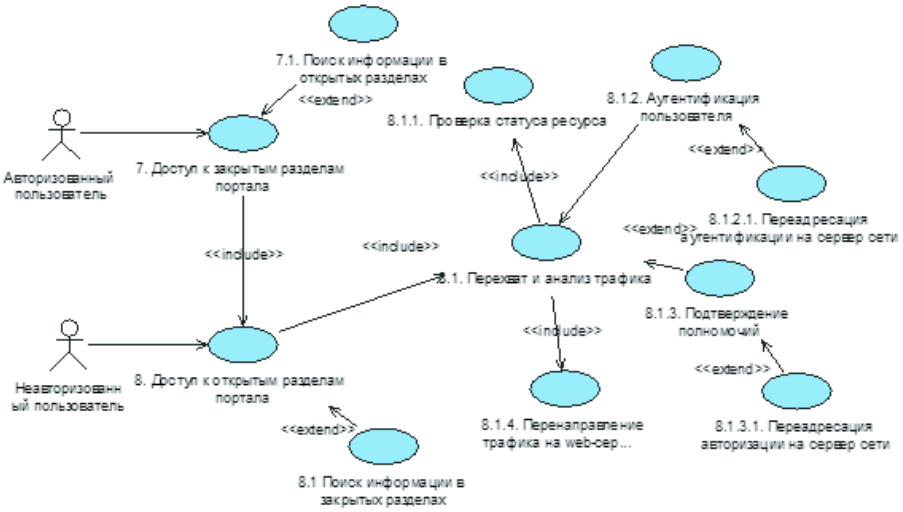


Рисунок 9 - Прецедентная модель функций обеспечения доступа к ресурсам порталов

Также не стоит забывать и о том, что, если проанализировать варианты применения подсистемы и построенных моделей вариантов, осуществляется обеспечение отчетливого выявления пользователей в соответствии с системой управления, осуществляется структурирование функциональных требований в соответствии с системой, точное очерчивание ее границ и сущность подсистемы того, как разделяется перекрестный доступ, в результате чего система разрабатывается в сопровождении с достаточно эффективным процессом.

3.4 Управление перекрёстным доступом к информационным ресурсам корпоративных порталов

Для пользователя характерно получение доступа в соответствии с информационными ресурсами, если заданы права и выбраны правила, как только были созданы пользовательские домены и интегрированы в сеть информационные ресурсы после аутентификации и авторизации в соответствии с системой.

Далее, следует осуществить рассмотрение следующих правил:

– входящий трафик на сервер в соответствии с протоколом HTTP перехватывается в соответствии с обратным проксированием;

– необходимо проанализировать то, чему принадлежит пользовательский запрос в соответствии с конкретным разделом портала и проверить то, имеется или отсутствуют ограничения в соответствии с доступом к ИР;

– в соответствии с открытостью ресурса, предоставление доступа осуществляется в соответствии со всеми пользователями, когда перенаправляются пользовательские запросы до *web*-сервера портала;

– проверка в соответствии с закрытым ресурсом возможности распознавания пользователя в системе. При отсутствии возможности распознавания для системе характерно выдвигать предложение пользователю пройти аутентификацию, используя имя и пароль;

– система проверяет доступ в соответствии с запрашиваемым ресурсов, если осуществляется аутентификация пользователя;

– при подтверждении пользовательских полномочий осуществляется предоставления доступа в соответствии с запрашиваемым ресурсом, когда перенаправляется запрос на web-сервер портала, когда включен в запрос IP-адрес [3.]

Последователь того, как система определяет пользователя, осуществляется в соответствии с рисунком 10.

Рисунок 10 составлен для более удобного схематичного представления того, как идентифицируется пользователь в соответствии с перекрестным доступом.

При верном ведении ID и пароля, для системы характерно осуществлять открытие и отображение базовой экранной формы. В другой ситуации пользователь получает сообщение о том, что данные для входа введены неверно, после чего предоставляется повторная возможность идентификации.

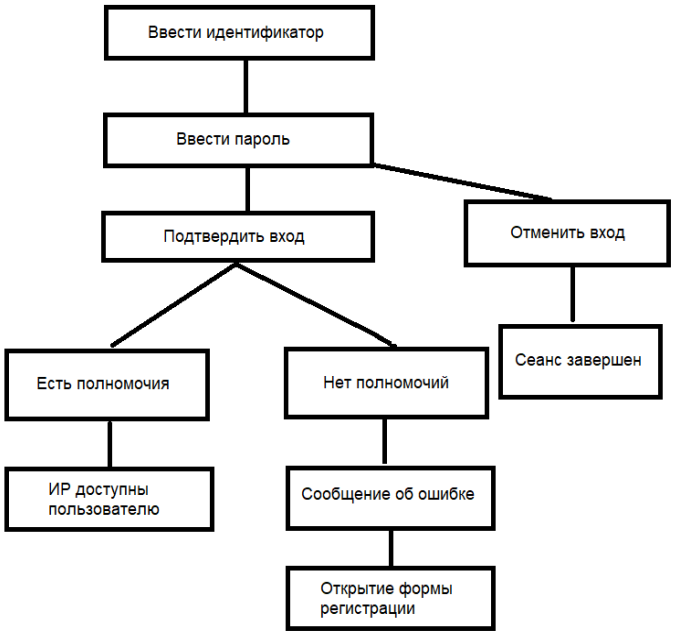


Рисунок 10 - Идентификация пользователя в подсистеме разграничения перекрёстного доступа

Как только открывается базовая экранная форма, для пользователя характерно получение доступа в соответствии с информационными ресурсами по привилегиям доступа.

Для пользователя предусматривается право отмены входа в любой момент, в результате чего осуществляется завершение рабочей сессии в системе.

Серверы управления доступом позволяют аутентифицироваться и авторизоваться каждому пользователю. Для отдельных серверов доступа характерно хранение всех данных пользовательских доменных категорий.

При обращении пользователя в соответствии с ресурсом посредством сторонней группы доменов, для сервера характерна переадресация запроса в соответствии с центральным сетевым сервером.

В результате этого осуществляется формирование требования в том, чтобы хранить пользовательскую информацию в соответствии с базами

данных, когда также присутствует возможность получить доступ в соответствии с разнообразными узлами.

3.5 Методика управления перекрёстным доступом к информационным ресурсам сети корпоративных порталов ООО «ИЦ АЙ-ТЕКО»

Разработка эффективного способа, чтобы контролировать перекрестный доступ в соответствии с корпоративными порталами рассматриваемой в текущей работе организации, осуществляется в соответствии с тем, если когда для разработчика характерно наличие отчетливого понимания и формального описания целой структуры объекта управления – какие имеются связи элементов системы, каковы особенности структуры в соответствии с информационными ресурсами, а также какие действуют правила того, как взаимодействуют между собой и функционируют компоненты системы.

В формате иерархии системы моделей удобно осуществлять исследование модели по информационному взаимодействию.

В соответствии с первоначальным уровнем осуществляется анализ того, как пользователь и система взаимодействуют друг с другом, когда предоставляются пользователю определенные услуги.

Для верхнеуровневых моделей характерно детального описания реализации процессов в соответствии с определенной базовой моделью с охватом технических, организационных или организационных технических факторов контакта.

Пользователь системы выступает в качестве человека или технического устройства, которое имеет способность в отправлении запросов в соответствии с системами посредством телекоммуникационных каналов связи с получением ответа в качестве того, что был предоставлен

соответствующий доступ в соответствии с конкретным ресурсом или последовал отказ.

В данном случае юзер относится только к одной организации, которая входит в состав сети порталов.

Также необходимо ввести фиктивную организацию для внешних пользователей, не принадлежащих ни к одной из организаций. Особенностью таких пользователей является равнозначные права и самый низкий уровень доступа.

Для пользовательского домена характерно формирование большого количества пользователей, регистрация которых осуществляется в качестве участника поддерживаемой организации.

Для доменов предусматривается разделение в соответствии с поддоменами, в результате чего осуществляется формирование непересекающихся друг с другом множеств или иерархии [3.]

Домен в соответствии с такой иерархией разбивается лишь в соответствии с таки доменом, а доступ имеют лишь его участники.

Рисунок 11 составлен для более наглядного схематического представления того, в какой последовательности исполняют операции по контакту пользователя и системы.

Обозначение физических устройств, информации, которая запрашивается пользователем, осуществляется в соответствии с ресурсом.

Для информации в таком случае характерно выступать в качестве всей информации по системе.

Для физического устройства характерно выступать в качестве сервера, который осуществляет обеспечение передачи ресурса до пользователя.

Когда пользователь авторизуется до того момента, как он получает идентификатор сессии, осуществляется его передача до сервера наименований, в результате чего формируется уведомление о том, что пользователь авторизован для всех остальных серверов доступа [3.]

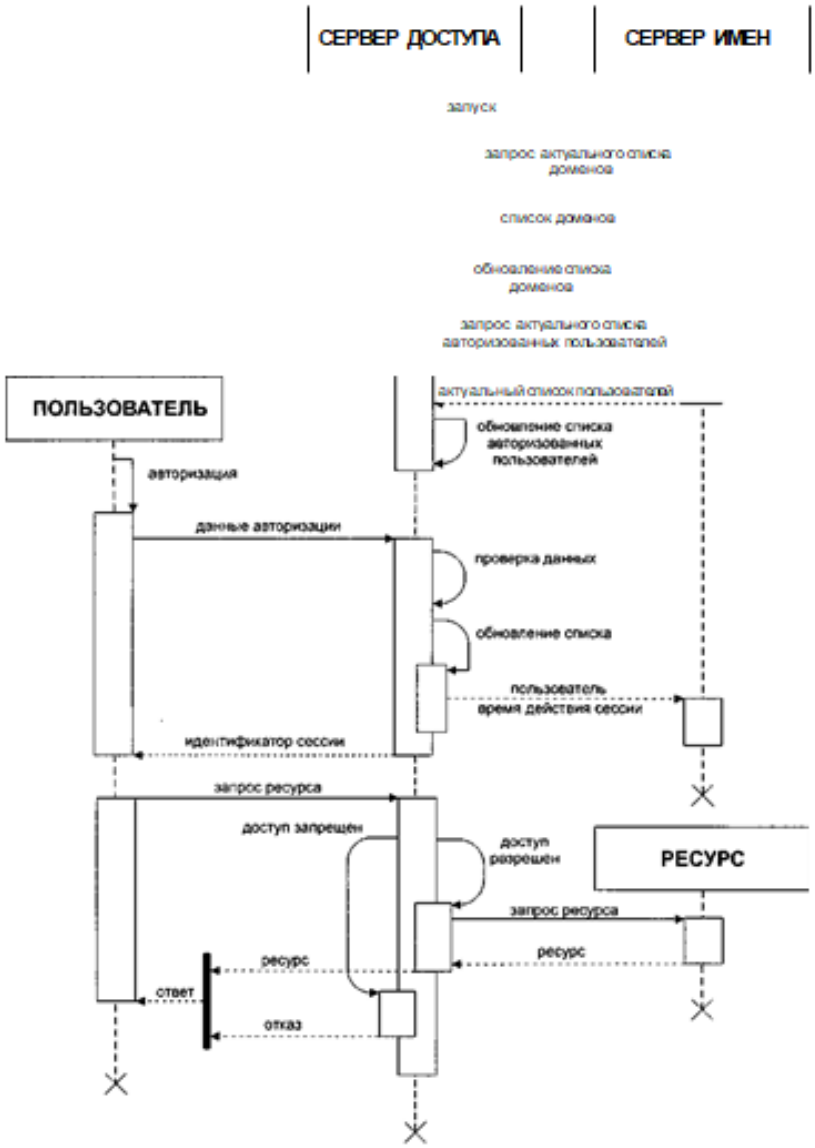


Рисунок 11 - Диаграмма последовательности взаимодействия пользователя с системой

После того, как предоставляется ID сессии для пользователя, осуществляется формирование критичного момента, поскольку для пользователя характерно осуществить обращение в соответствии с ресурсами, которые еще не подвергались обновлению.

В результате этого пользователь получает отказ в доступе, даже если у него имеются достаточные привилегии.

Чтобы решить такую задачу запрещается задерживать выдачу пользователю ID сеанса до тех пор, пока не будет сформировано наличие подтверждения, так как в результате этого осуществляется формирование слишком большого периода ожидания, а формирование системы осуществляется так, что она будет выступать в качестве наиболее чувствительной, если последует отказ.

В результате этого в обязательном порядке требуется обеспечение достаточной вероятности отказа для пользователя в предоставлении услуги доступа и смещение такой ситуации в соответствии с увеличением скоростью, с которой отвечала бы система.

Перекрестный доступ управления ИР в обязательном порядке предоставляет и определяет то, в каком содержании находится объект управления и его состояния [3].

Рисунок 12 составлен для более удобного представления того, в какой последовательности должны осуществляться действия, чтобы решить основные системные задачи.

Корпоративные порты в сети выстраиваются в соответствии с предложенной моделью в качестве процесса, который направлена на представление собственных участников, последовательности операций, в качестве функционирующей сети в соответствии с корпоративными порталами рассматриваемой в текущей работе организации.

Первая стадия характеризуется выделение участников процесса, в соответствии с которыми корпоративный портал в сеть, другими словами – наличие владельцев и порталов сети и пользователей.

Владельцы корпоративного портала формируют структура портала в соответствии с рассматриваемым узлом, осуществляют управление и контроль учетных записей группы доменов, контролируют то, как функционирует доступ в систему и ресурсы [3.]

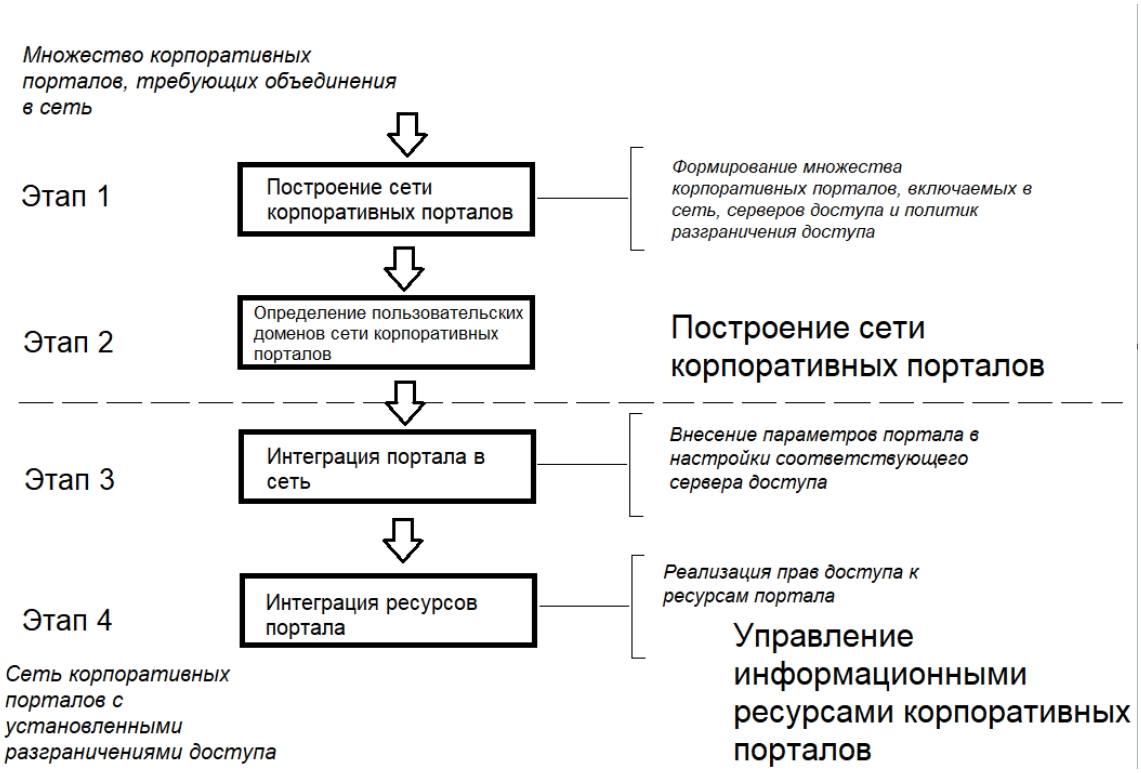


Рисунок 12 - Методика управления перекрёстным доступом к ИР в сети корпоративных портало

В качестве фундаментальных задач в соответствии с центром управления сетью корпоративного портала рассматриваемой в текущей работе организации, выступает:

– управляются доменные группы;

– распределяются административные обязанности;

– управляется доступ в соответствии с доменными группами;

– контролируются репликации данных и то, насколько корректно функционирует сеть.

Для пользователей сети характерно поиск решений для того, чтобы решить следующие задачи:

– распределение ролей в соответствии с каждым участником группы;

– подписание соглашений между каждыми участниками группы;

– охарактеризованы каналы взаимодействия;

– информационные ресурсы должны быть оценены в соответствии с объемами;

– определение критериев и того, как классифицируются ресурсы.

Детально представление последовательности, в соответствии с которой необходимо выстраивать сеть, осуществляется в соответствии с рисунком 13.

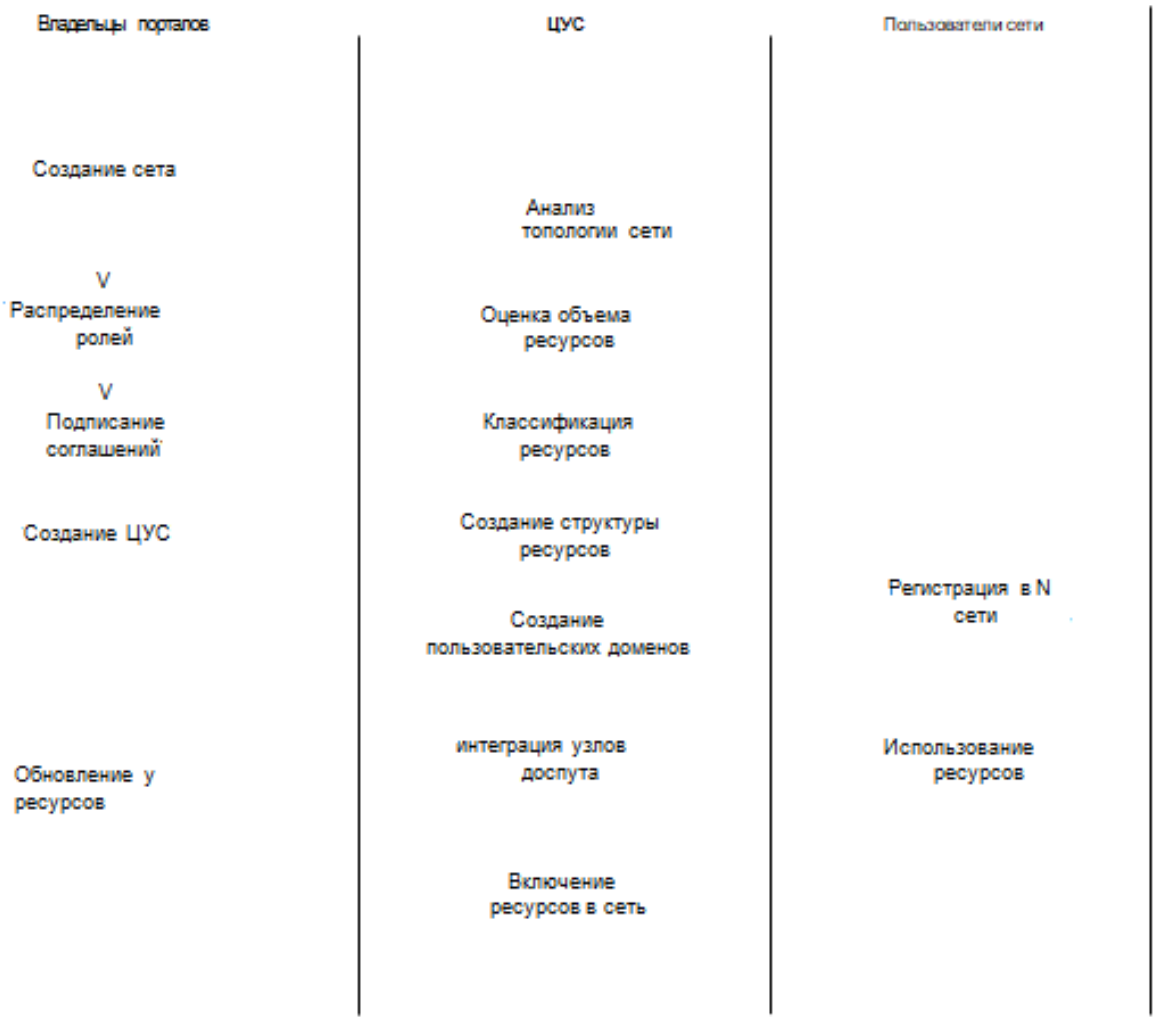


Рисунок 13 - Алгоритм построения сети корпоративных порталов

Детально представление последовательности, в соответствии с которой необходимо выстраивать сеть, осуществляется в соответствии с рисунком 13.

Требуется осуществить формирование правил, в соответствии с которыми, далее, осуществляется реализации подсистемы управления

доступам к ИР когда рассматриваются корпоративные порталы ООО «ИК И-ТЕКО»:

1. Для портала характерно выступать в качестве системы, в которую входят связанные друг с другом разделы с иерархической древовидной структурой подчиненности, где для каждого объекта характерно наличие одного родительского и неограниченного количества дочерних.

2. Для каждого раздела предусматривается наличие связи с защищенным ресурсом, применяя конкретную ссылку URL [3.]

3. Каждый раздел характеризуется единственным и уникальным правилом доступа.

В соответствии с родительскими объектами стоит отметить наличие возможности в управлении связанными друг с другом объектами вторичного или дочернего порядка. Другими словами, когда для родительского объекта предоставляется доступ, то такой доступ автоматически предоставляется и дочернему объекту.

В соответствии с каждым наследником присутствует возможность отключения инструмента, с помощью которого назначается последующее правило, которые не распространяется в соответствии с родительским объектом.

4. Чтобы сформировать новое правило доступа в соответствии с разделом, для группы привилегий характерно наличие уровня, не ниже, чем у родительского объекта. В результате этого пользователь, у которого повышенный уровень привилегий, характеризуется наличие доступа в соответствии с разделами, к которым требуется доступ привилегий ниже [3.]

5. Осуществляется выделение 16 уровней привилегий доступа в рассматриваемом в текущей работе портале. Сущность нулевого уровня состоит в том, что для раздела характерно выступать в качестве общедоступного. И, чтобы разграничить права доступа в соответствии с защищенными разделами порталов, осуществляется представление уровня 1-16.

6. Пользователи разделяются в соответствии с непересекающимися подмножествами, применяя группу привилегий доступа. Другими словами, для пользователя характерно обладать принадлежностью в соответствии с одной группой привилегий доступа [34.]

7. В соответствии с любым сеансом осуществляется присвоение ID авторизованного пользователя сеанса, который выступает в качестве уникального набора. Благодаря идентификатору осуществляется предоставление прав для пользователя посредством процесса, когда идентификатор распознается по запросу пользователя на портале.

На второй стадии формулируются фундаментальные функциональные задачи для каждого системного администратора. В качестве таких задач выступают:

1. Управлять сетью портала посредством того, что создаются группы пользователей домена, устанавливаются права доступа между группами доменов с формирование уровня прав доступа.

3. Управляются пользовательские учетные записи.

4. Контролируется работа сети и то, как обмениваются информацией пользователь и сервер [3].

В соответствии с правилами, по которым осуществляется администрирование, осуществляется определение членов и функций администраторов с последовательностью того, как они должны действовать.

Когда сеть изменяется или формируется, изначально для администратора характерно формирование пользовательского домена, для которого предусматривается его связь с доменом члена портала в Интернете.

Администратор выполняет ключевую задачу, которая направлена на то, чтобы определить количество групп участник в соответствии с привилегиями доступа, а также определить сетевые администраторы.

Для доменного администратора характерно формировать пользовательскую базу данных, реализация которой осуществляется в соответствии с методами, представленными ниже:

- интегрировать и связывать сервер доступа в соответствии с корпоративным сервером авторизации,

- применять существующее хранилище корпоративной информационной системы, после чего импортировать пользовательские учетные записи,

- регистрировать пользователей, применяя инструменты в соответствии ч ручным администрированием.

Далее, для администратора доступа характерно осуществлять интегрирование информационных ресурсов члена в соответствии с сетью портала с формирование требуемых решений.

Рисунок 14 представлен для более удобного понимания алгоритма.

Рисунок 14 - Алгоритм определения пользовательских доменов сети корпоративных порталов

На рисунке 14 схематично показан алгоритм определения доменов пользователей сети корпоративного портала

Третья стадия способа характеризуется тем, что здесь организуется информационная связь, интегрируются участники в соответствии с ИК-сетью.

Корпоративный портал выстраивается в соответствии с тем, что формируется база данных ресурсов, как карта сайта в соответствии с серверами доступа.

Для одного пользовательского домена характерна связь с многочисленными доменами интернет портала [3].

Для администратора портала характерна изначальная интеграция доменного наименования в соответствии с сетью портала, предусматривая связь участника в соответствии с конкретным доменом пользователя и перекрестным доступом, так как предоставления серверного доступа проводится посредством того, что применяется уникальный идентификатор URI, где в качестве основного элемента выступает наличие доменного наименование портала в соответствии с URL-адресом.

Также осуществляется формирование требуемых описаний и информационного дайджеста.

Третья стадия характеризуется добавление информационного ресурса в соответствии с корпоративными порталами рассматриваемой в текущей диссертационной работе организации, где осуществляется установка соответствующих разрешений.

При этом стоит отметить наличие изменений прав доступа с разрешительного доступа на запретительный, в соответствии с которым отмечается наличие завышенного приоритета [3].

Выводы к главе 3

В 3 главе определено, что способ, в соответствии с которым управляются корпоративные порталы, характеризуется предоставлением в таком случае субъектами доступа ролей для пользовательского исполнения. Для самих прецедентов характерно выступать в качестве таких действий, которые производились бы на информационном ресурсе корпоративного портала.

Для каждого прецедента характерно выступать в качестве законченного потока явлений в соответствии с подсистемой, где разграничивается доступ в соответствии с корпоративными порталами рассматриваемой в текущей работе организации.

Для преодоления препятствий в работе системы, осуществляется структурирование объектных моделей системы так, что для каждой характерно выступать в качестве отдельного фактора ее применения.

В соответствии с применяемой методикой стоит отметить, что каждый фактор обладает соответствием в соответствии с одним прецедентом системы в целом, он описан только теми объектами, который выступают в качестве участника такого прецедента.

Применение объекта осуществляется в соответствии с разнообразными прецедентами.

Когда исследуется предложенная методика, осуществляется определение следующих практических ограничений:

– для корпоративного портала характерно наличие системы управления контентом;

– осуществляется учет физического подключение сервера, с помощью которого обслуживается корпоративный портал и имеется возможность к тому, чтобы подключить сервер доступа;

– возможно временно отказывать в соответствии с обслуживанием на иерархии провайдера.

Также осуществляется представление фундаментальных участников процесса, в соответствии с которым формируется сеть в соответствии с корпоративными порталами и их ключевыми задачами:

– владельцы порталов сети формируют структура портала, управляют и контролируют учетные пользовательские записи, контролируют то, как функционирует узел системы доступа и обращения в соответствии со связанными друг с другом порталами;

– центр управления сетью корпоративных порталов ООО «ИЦ АЙ-ТЕКО» осуществляется управление и контролирует доменные группы, делегирует администраторские полномочия, контролирует доступ в соответствии с группами домена, контролирует то, как функционирует вся сеть, а также реплицирует данные;

– пользователи сети получают доступ в соответствии с открытыми разделами портала и авторизованный доступ в соответствии с закрытыми разделами корпоративного портала.

Проведена разработка алгоритмов, в соответствии с каждой стадией рассматриваемого способа.

Глава 4 Разработка подсистемы разграничения перекрёстного доступа к информационным ресурсам в сети корпоративных порталов ООО «ИЦ АЙ-ТЕКО»

4.1 Применение диаграммы развертывания подсистемы разграничения перекрёстного доступа к информационным ресурсам в сети корпоративных порталов ООО «ИЦ АЙ-ТЕКО»

«При разработке корпоративных приложений таких диаграмм может быть полезно для решения задач использования компонентов, с целью использования распределенных вычислительных и коммуникационных сетевых ресурсов и обеспечения безопасности» [7].

«Диаграммы развертывания используются для представления общей конфигурации и топологии распределенной программной системы в нотации UML» [7].

«Схема развертывания предназначена для визуализации элементов и компонентов программы, существующих на этапе ее выполнения. В этом случае представлены только компоненты-экземпляры программы, которые являются исполняемыми файлами или динамическими библиотеками. Компоненты, которые не используются во время выполнения, не отображаются на схеме развертывания. Схема развертывания содержит графические изображения исполнительных модулей, устройств, процессов и связей между ними» [7].

Последним шагом в спецификации модели программной системы обычно является разработка схемы развертывания.

Существует 2 способа показать какие компоненты размещаются на отдельном устройстве, это возможно сделать двумя способами.

В первом случае - это разделение горизонтальной линией графики устройства на два участка, записывая вверху имя устройства и компоненты, размещаемые на этом узле.

«Второй способ показан на схеме развертывания устройства со встроенными образами процессов. Однако следует учитывать, что только исполняемые компоненты могут быть выполнены в качественных компонентах. Помимо имени узла, могут использоваться различные стереотипы, в которых явно указано назначение этого устройства» [7].

Для повышения уровня восприятия в диаграммах используются графические знаки, поясняющие устройство системы.

«Отношения зависимости между узлом и развернутыми на нем компонентами, также могут быть представлены на диаграмме, что является альтернативой вложенному изображению компонентов внутри символа узла. Разработка диаграммы развертывания начинается с идентификации всех аппаратных, механических и других типов устройств, которые необходимы для выполнения системой своих функций» [7].

4.2 Проектирование подсистемы разграничения доступа в сети корпоративных порталов предприятий

«Проектирование архитектуры программной реализации подсистемы разграничения доступа в сети корпоративных порталов предприятий будет осуществляться путём рассмотрения особенностей функционирования сети корпоративных порталов и схемы размещения оборудования; а так же распределения программных компонентов и служб между устройствами» [7].

Схема физического распределения и организации составных частей сети корпоративных порталов предприятий представлена на рисунке 15.

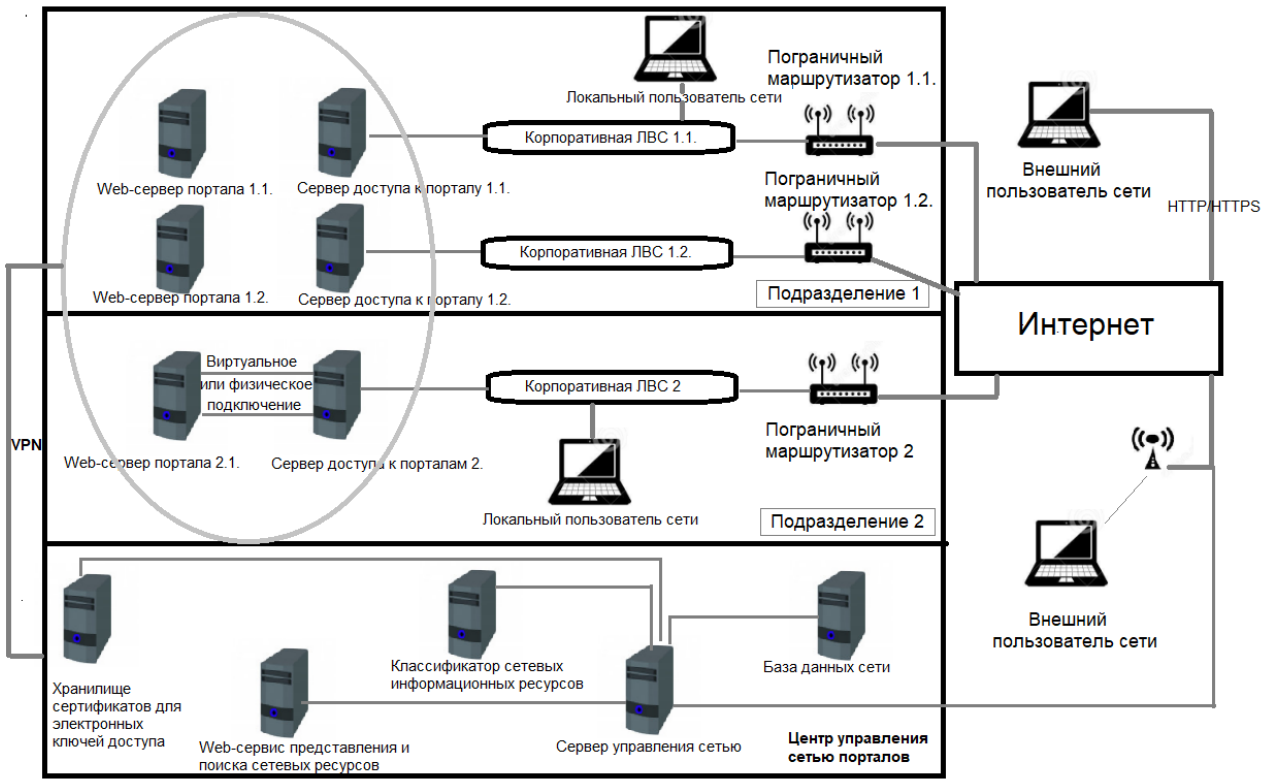


Рисунок 15 - Схема физического распределения и организации составных частей сети корпоративных порталов предприятий

Отличительными особенностям построения и функционирования системы являются:

«Компоненты подсистемы управления доступом функционируют на серверах доступа, отвечающих за пользовательский домен и ассоциированные с ними порталы. Сервера доступа, в свою очередь, связаны с центральным сервером управления сети (ЦУС). Каждый отдельный сервер доступа устанавливается в разрыв подключения Web-сервера к корпоративной сети и сети Интернет. Он выполняет функции маршрутизатора и брандмауэра и, соответственно, является для Web-сервера внешним шлюзом. Один сервер доступа может обеспечивать защищенный доступ к одному или группе порталов, работающих на одном или нескольких серверах, которые можно на логическом или физическом уровне отделить с помощью сервера доступа от других фрагментов сети» [21].

«На основе анализа схемы построения и функционирования

подсистемы разграничения доступа в сети корпоративных порталов предприятия, с учетом специфики реализации и, конечной целью создание технического решения в идее аппаратно-программной платформы, построена модель развертывания системы на основе UML» [24].

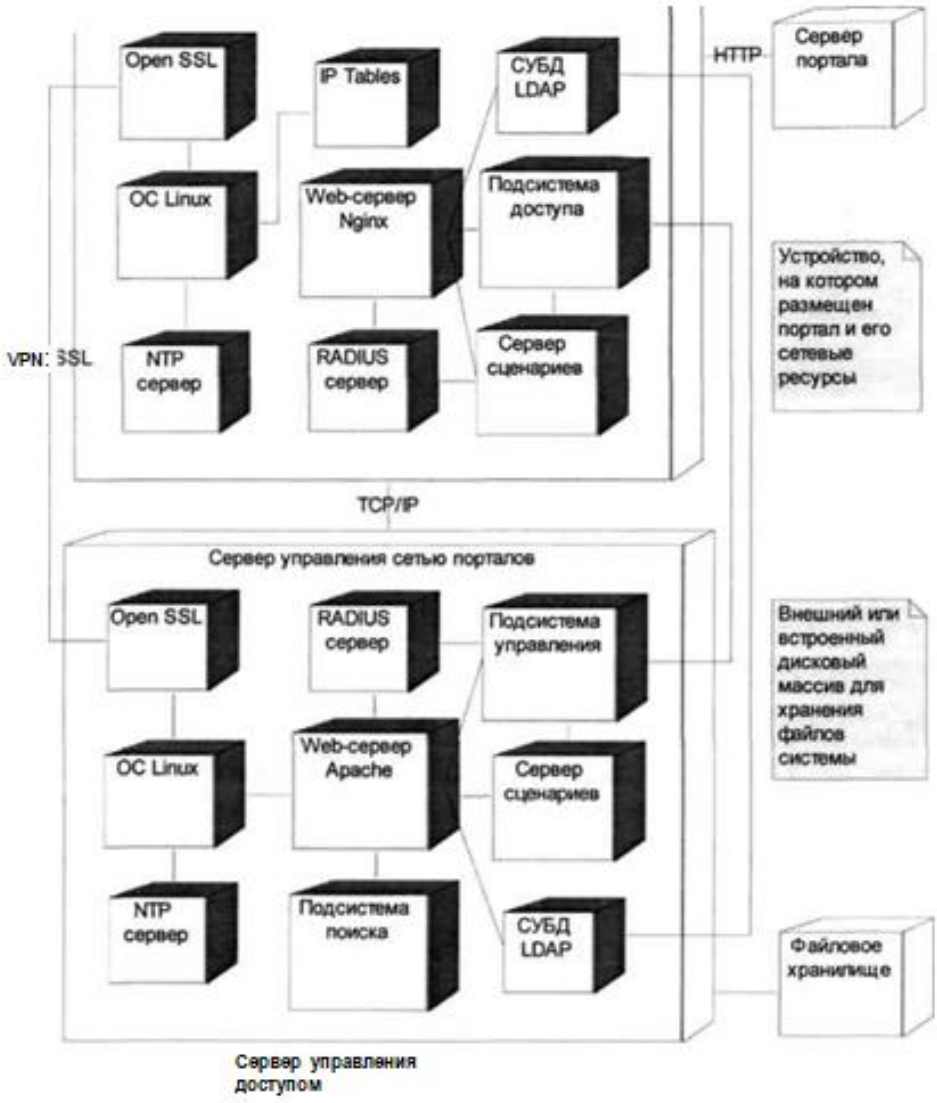


Рисунок 16 - Диаграмма развертывания системы

На рисунке 16, представлена модель в виде диаграммы развертывания системы, обеспечивая наглядное представление взаимосвязей составных элементов готовой системы.

Перечень и назначение используемых дополнительных компонентов и

служб для серверов управления доступом и управления сетью приведен в таблице 3.

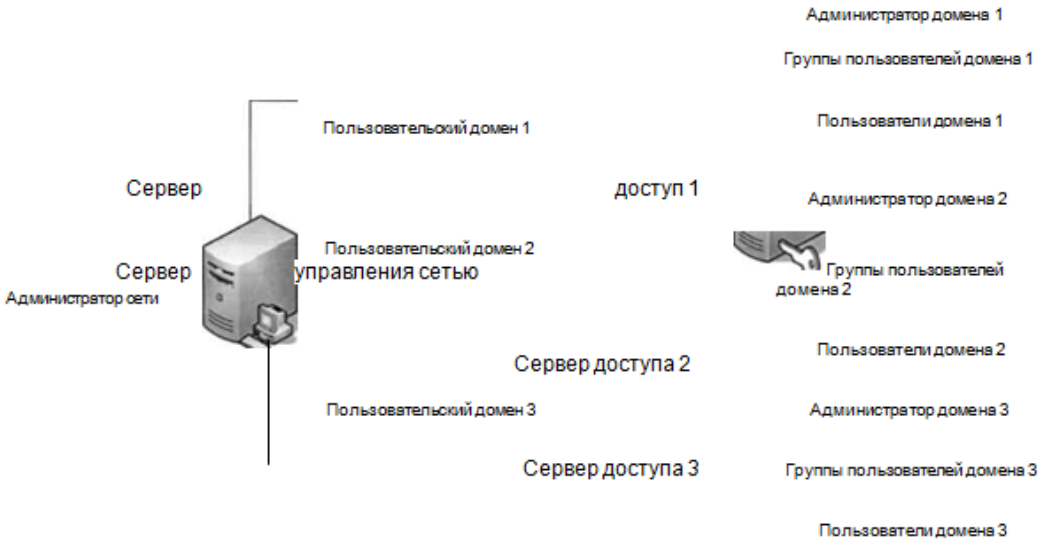
Таблица 3 – Перечень компонентов и служб серверов подсистемы разграничения доступа к ИР корпоративных порталов ООО «ИЦ АЙ-ТЕКО»

Наименование	Назначение
ОС Linux	Операционная система, в среде которой функционируют все программные компоненты подсистем
RADIUS-сервер	Служба аутентификации и авторизации, делает возможным использовать сервер доступа в качестве AAA сервера для других корпоративных системы
Web-сервер N	Программное приложение, обеспечивающее перехват и ретрансляцию пользовательских запросов к ресурсам порталов (обратный прокси)
СУБД LDAP	Программное приложение, обеспечивающее функционирование локальных баз данных сервера доступа
Сервер сценариев	Служба выполнения программных сценариев обработки запросов и других компонентов системы
Подсистема доступа	Все программные компоненты клиентской части системы, расположенные на сервере контроля доступа и реализующие функционал контроля доступа
Подсистема поиска	Программные компоненты и интерфейсы, выполняющие задачи классификации представления и поиска информационных ресурсов сети

Следует подчеркнуть, что было реализовано физическое представление подсистемы разграничения доступа сети корпоративных порталов ООО «ИЦ АЙ-ТЕКО».

Это является основой для построения оконченного технического решения в виде аппаратно-программной платформы для развертывания сетей корпоративных порталов.

На рисунке 17, представлена иерархия пользователей сети корпоративных порталов.



.

Рисунок 17 - Иерархия пользователей сети корпоративных порталов

4.3 Обратный прокси-сервер и его роль в системе

Описываемая концепция построения подсистемы разграничения перекрёстного доступа к ИР в сети порталов ООО «ИЦ АЙ-ТЕКО» призвана решать задачи обмена информацией между предприятиями и предоставления доступа к данным через Web-порталы в Интернет, обеспечивая при этом надежную защиту информации от несанкционированного доступа.

«Одним из вариантов является использование фронтального Web-сервера в качестве обратного прокси-сервера (reverse proxy- server). В этом случае обеспечивается включение дополнительного устройства между сетью Интернет и основным Web-сервером» [29].

«В современной практике проектирования и построения информационных систем стандартом стал объектно-ориентированный подход, позволяющий выделить повторяющиеся архитектурные конструкции - шаблоны проектирования (design pattern)» [29].

4.4. Шаблоны проектирования описывающих обратный прокси-сервер

В работе приводится несколько шаблонов проектирования реализующих обратный прокси-сервер в различных контекстах. Эти шаблоны выходят за рамки простых шаблонов, но в тоже время не описывают необходимую функциональность.

«Следовательно, необходимо, ориентируясь на существующие и применяемые при проектирование и программной разработке шаблоны, встроить в систему фронтальный Web-сервер» [29].

В данной ситуации целесообразно использовать фронтальный Web-сервер (здесь выступает как обратный прокси-сервер в контексте обеспечения безопасности, security reverse proxy).

Таблица 4 – Покомпонентное описание схемы с использованием обратного прокси-сервера в контексте обеспечения безопасности

Компонент	Выполняемые действия	Взаимодействие
Брандмауэр	Фильтрация входящего сетевого и пропуск только соответствующего типа трафика (HTTP).	Обратный прокси-сервер. Клиент.
Обратный прокси-сервер	Разрешение запросов от клиента и передача только валидных запросов внутреннему Web-серверу. .	Внутренний Web-сервер.
Внутренний Web-сервер	Осуществление действительного Web-функционирования.	Обратный прокси-сервер. Клиент.

«Обычно Web-портал конструируется из различных компонентов и требует различного программного окружения (несколько серверов приложений или наборов сценариев)»[29].

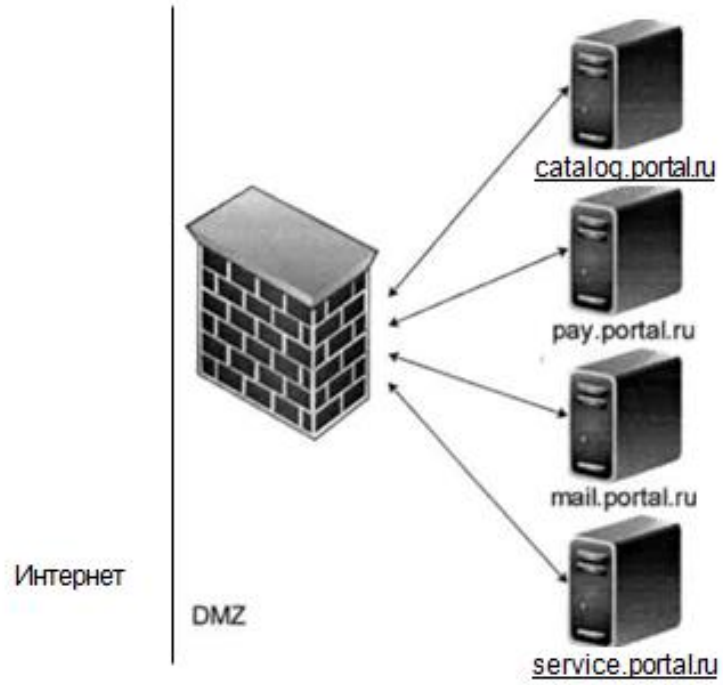


Рисунок 18 – Типичная структура Web-портала

На рисунке 18 можно заметить, что разделение зачастую происходит на уровне доменов в URI (Uniform Resource Identifier – унифицированный идентификатор ресурса), т.е. различные компоненты портала доступны по определенным URI.

«В этой ситуации возникают следующие задачи:

– объединение ПО различных разработчиков в рамках Web-портала.

– сокрытие от клиента внутренней структуры Web-портала.

– сохранения целостности гиперссылок в рамках Web-портала, при реорганизации.

– возможности балансировки нагрузки на серверы.

– возможность использования единого SSL-сертификата для различных сервисов Web-портала.

Для решения поставленных задач целесообразно организовать взаимодействие с использованием единого интегрирующего обратного

прокси-сер-вера. Данных подход даёт возможность решить все указанные выше задачи» [20].

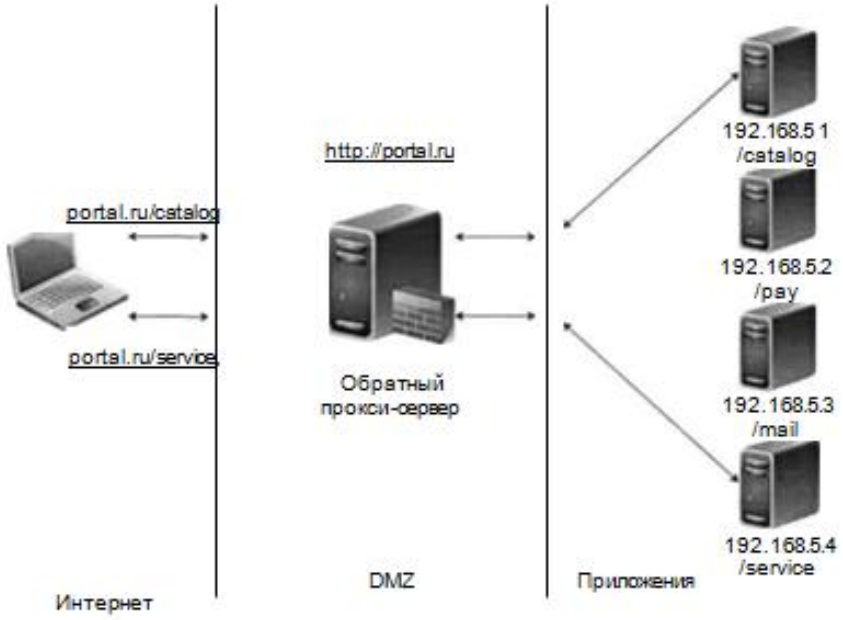


Рисунок 19 - Структура портала с использованием интегрирующего обратного прокси-сервера

На рисунке 19 представлен интегрирующий обратный прокси-сервер (integration reverse proxy).

«Развитием описанного шаблона может быть делегирование дополнительных функций обратному прокси-серверу, например: аутентификация, авторизация, управление сеансами пользователей.

В этой ситуации обратный прокси-сервер используется как точка единого входа (front door, single sign-on).

К основным функциональным задачам, решаемым обратным прокси-сервером относятся:

– поддержка сеансов пользователей (включая аутентификацию, авторизацию и аккаунтинг).

– фильтрация и перенаправление запросов.

– возможности балансировки нагрузки на серверы.

– возможность использования единого SSL-сертификата для различных сервисов Web-портала»[15].

Исходя из списка функциональных задач, можно сделать вывод о том, что адекватным будет применение шаблона проектирования – точка единого входа.

4.5 Выбор архитектуры программно-технического комплекса взаимодействия распределенных компонентов подсистемы разграничения доступа в сети корпоративных порталов

В этой главе диссертационной работы, предполагается предложение архитектуры программно-технического комплекса на платформе свободно распространяемого ПО, обеспечивающего эффективное разграничение перекрёстного доступа к ИР корпоративных порталов в сети ООО «ИЦ АЙ-ТЕКО» через открытые каналы Интернет. Что, в свою очередь, обуславливает решение задачи: обеспечение безопасного, надежного и эффективного взаимодействия распределенных компонентов подсистемы разграничения перекрёстного доступа между собой.

С этой целью необходимо провести анализ типа и характера информационного взаимодействия с целью определения применимости различных протоколов для организации взаимодействия компонентов системы.

4.5.1. Анализ информационных потоков межу компонентами подсистемы разграничения доступа

На этапе проектирования архитектуры системы необходимо рассмотреть информационные потоки в рамках подсистемы разграничения

перекрёстного доступа к ИР в сети корпоративных порталов ООО «ИЦ АЙ-ТЕКО».

В таблице 5 перечислены потоки данных, с указанием их особенностей и требований по обеспечению безопасности.

Таблица 5 – Особенности информационных потоков внутри подсистемы разграничения доступа

Компонент 1	Компонент 2	Среда взаимодействия	Требуется повышенная безопасность взаимодействие	Передаваемые данные
Фронтальный Web-сервер	Внутренний Web-сервер	Локальная сеть	Нет	Данные запроса в рамках протокола HTTP(S)
Сценарий перенаправления	Фронтальный Web-сервер	Локальная сеть/Общая	Нет	Данные запроса в рамках протокола HTTP(S)
Сценарий перенаправления	Внутренний Web-сервер	Локальная сеть	Нет	Данные запроса в рамках протокола HTTP(S)
Сценарий поддержки сеанса пользователя	AAA-сервер	Локальная сеть	Да	Данные в рамках протокола AAA-сервера
AAA-сервер	СУБД	Локальная сеть	Да	SQL-инструкции на выборку и данные о пользователях и их правах доступа
Клиент	Фронтальный Web-сервер	Глобальная сеть Интернет	Да	Аутентификация, авторизация, учёт деятельности, выдача и редактирование информационного содержимого порталов, и т.п.

4.5.2. Каналы взаимодействия компонентов подсистемы разграничения перекрёстного доступа к информационным ресурсам

«При взаимодействии клиента со сценарием поддержки сеанса пользователя, который выполняется после поступления соответствующего инициирующего HTTP-запроса, происходит автоматическое переключение взаимодействия на безопасный канал коммуникации. Вслед за этим фронтальным Web-сервером открывается сеанс работы по защищенному протоколу HTTPS. В свою очередь запросы к СУБД на получение и проверку идентификационных данных пользователя и идентификатор сеанса могут выполняться по защищенному каналу, чтобы обеспечить безопасность в локальной сети организации»[11].

«Кроме безопасности информационного обмена можно указать как основное требование к системе в целом *высокую доступность (High Availability).* Доступность означает возможность группе пользователей использовать систему»[12].

Если у них нет такой возможности, система считается недоступной.

4.5.3. Протоколы для взаимодействия компонентов подсистемы разграничения доступа в сети корпоративных порталов

«Решая задачу организации информационных потоков, следует рассмотреть существующие протоколы информационного обмена, задачи по обеспечению достаточного уровня защищённости с архитектурой системы.

Существуют альтернативные пути организации защищенных туннелей для взаимодействия компонентов системы:

– туннелирование соединения на конкретный TCP-порт с помощью Stunnel (основан на SSL);

– использование IPSec решений»[28].

В таблице 6 приводится сравнение реализации функций разграничения доступа для наиболее широко используемых протоколов IPSec и SSL.

Таблица 6 – Особенности информационных потоков внутри подсистемы разграничения

Особенности	IPSec	SSL
Аппаратная независимость	Наличествует	Наличествует
Применимость для приложений	Не требуется изменений для приложений	Не требуются изменения в приложениях
Защита	IP пакет целиком; включает защиту для протоколов высших уровней	Только уровень приложений
Производительность	Меньшее число переключений контекста и перемещения данных	Большее число переключений контекста и перемещения данных.
Платформы	Любые системы, включая роутеры	В основном, конечные системы (клиенты/серверы)
Firewall/VPN	Весь трафик защищен	Защищен только трафик уровня приложений. ICMP, RSVP, QoS и т.п. могут быть
Прозрачность	Для пользователей и приложений	Для пользователей и приложений (при дополнительной настройке)
Текущий статус	Появляющийся стандарт	Широко используется WWW браузерами, также используется некоторыми другими продуктами

«Отметим, что существует несколько протоколов обеспечения функционирования AAA-функционала.

Примерами являются протоколы RADIUS, TACACS+ и DIAMETER.

В рамках системы предпочтение целесообразно отдать протоколу RADIUS так как:

– протоколы TACACS+ и DIAMETER являются функционально перегруженными, следовательно, более требовательными к вычислительным ре-

сурсам, что влечёт большее время отклика, а это в свою очередь является критическим показателем для системы;

– протокол RADIUS работает на основе транспортного протокола UDP, что делает его более быстродействующим (DIAMETER и TACACS+ используют TCP);

– протокол RADIUS позволяет перенаправлять запросы от одного RADIUS-сервера к другому.

Следует отметить, что в проведенном анализе взаимодействия распределенных компонентов системы определены специфика и требования к внутренним коммуникационным каналам. Исходя из этого, определены требования и сформировано подмножество соответствующих им протоколов, которые целесообразно применять»[30].

4.6. Экспериментальный образец и проведение оценки показателей эффективности

Объединение корпоративных порталов в сеть дает ряд эффектов: организационный; социальный; экономический.

«Организационный эффект заключается в изменении процессов аутентификации и авторизации и разграничении полномочий в рамках сети корпоративных порталов, что позволяет сократить вероятность появления ошибок аутентификации и авторизации первого и второго рода.

Социальный эффект заключается в улучшении условий труда и снижении механической нагрузки на работника.

Экономическая эффективность для предприятия (или группы предприятий, объединяющихся в ассоциацию или отрасль) оценивается, начиная от момента времени, когда возникает необходимость в объединении корпоративных порталов в сеть или иную агрегирующую структуру»[30].

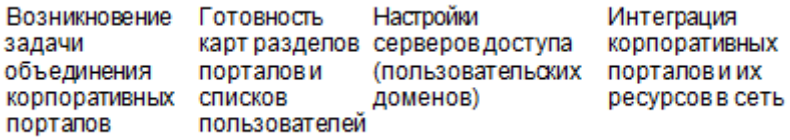


Рисунок 19 - Этапы процедуры развёртывания сети корпоративных порталов

На рисунке 19, определены этапы объединения можно представить в виде последовательности шагов (в соответствии с методикой описанной ранее) представленной хронологически.

Этапы реализации сети корпоративных порталов, возможно, соотнести с этапами реализации объединённого портала, таблица 7.

Таблица 7 – Этапы организации сети корпоративных порталов и объединённого портала

Интервал	Сеть корпоративных порталов	Объединённый портал
***h* — t_0**	Подготовка карт порталов. Создание списков пользователей.	Подготовка карт порталов Подготовка подразделов в рамках выбранного решения по организации объединённого портала
h*-*h	Настройка сетевых параметров серверов доступа. Ввод доменов пользователей.	Резервирование вычислительных ресурсов и пропускной способности каналов Настройка сетевых параметров объединённого портала Разработка (адаптация) необходимых портов
t3-t2	Интеграция на уровне административных ролей различного уровня (портала, сервера доступа, сети) Синхронизация данных с ЦУС	Интеграция средства реализации требуемой функциональности для подразделов объединённого портала

«На первом этапе подготовкой карт разделов порталов понимается построение иерархий разделов сайта с достаточной глубиной детализации, с возможностью представления в форматах (XML, JSON и т.п.).

На втором этапе под вводом доменов пользователей предполагается пакетный ввод пользовательских данных (имя домена, идентификаторы, аутентификаторы, роли, уровни привилегий и т.п.) в виде XML либо JSON для каждого сервера доступа. Сетевые настройки объединённого портала могут включать в себя необходимость балансировки нагрузки (load balancing).

На третьем этапе под интеграцией на уровне административных ролей предполагается внесение или редактирование данных о привилегиях администраторов разных уровней на сервера доступа и ЦУС»[31].

4.6.1. Оценка временных показателей по указанным интервалам

«Была осуществлена оценка и сравнения временных затрат на разграничение доступ при построении сети корпоративных порталов и при организации объединённого портала. Оценку временных и трудовых показателей для сети корпоративных порталов и объединённого портала получим с помощью одной из алгоритмических моделей оценки стоимости разработки программного обеспечения The Constructive Cost Model 2 (COCOMO 2). Данный способ оценки использует регрессионную формулу с параметрами, собранными из базы данных на основе статистической информации о многих проектах аналогичного класса»[7].

«Согласно данной модели трудозатраты рассчитываются следующим образом: Трудоёмкость: L (человеко-месяцев). Длительность разработки: T = q • (L) (месяцев). Число разработчиков: $D = L/T$ (человек).

Коэффициенты принимают следующие значения, в рамках данного метода оценки: a = 3.0, b = 1.12, q, = 2.5, db = 0.35.

Общий объем разработки объединённого портала оценочно может достигать 100 тысяч (значимых или логических) строк кода - параметр *KLOC* (kilo lines of code).

Таким образом, получаем следующие значения:

$Limportai = 3.0 \cdot (100)^{112} = 521.34$ (человеко-месяцев),

$Timportai = 2.5 \cdot (521.34)^{035} = 22.33$ (месяцев),

$Dimpartai = 521.34/22.33 = 23.34$ (человек).

Общий объем прототипа подсистемы разграничения доступа в сети корпоративных порталов, включающий в себя ЦУС и сервер доступа может быть оценён как — 40 тысяч (значимых или логических) строк кода.

Таким образом получаем следующие значения:

$L = 3.0 \cdot (40)^{112} = 186.82$ (человеко-месяцев),

$T = 2.5 \cdot (186.82)^{0.35} = 15.6$ (месяцев),

$D = 186.82/15.6 = 11.98$ (человек)»[18].

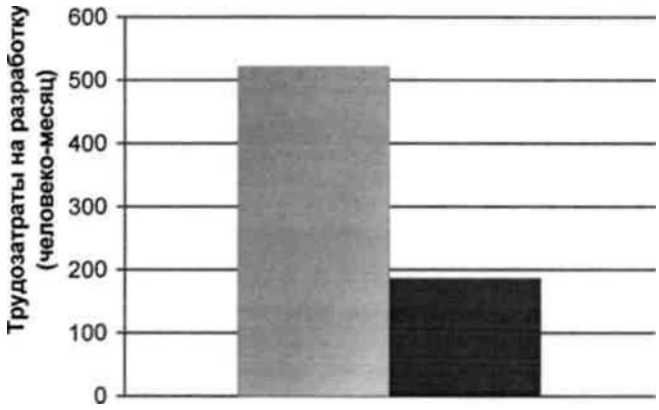


Рисунок 20 - Затраты на разработку подсистемы разграничения доступа в сети корпоративных порталов и создание объединённого портала

На рисунке 20, отражены сведённые расчётные данные методики COCOMO 2.

«Рассмотрим временные затраты на организацию введения дополнительного корпоративного портала в сеть и дополнительного раздела

объединённого портала ранее реализованного как отдельный корпоративный портал.

Представим динамику изменения временных затрат на графике зависимости от количества корпоративных порталов включаемых в агрегирующую структуру (сеть или объединённый портал). Обозначим количество порталов через *p*. Дополнительные расходы, в которые для сети корпоративных порталов войдёт развёртывание ЦУС b = 80 (человеко-часов), и первичная настройка объединённого портала b = 30 (человеко-часов)»[34].

Рисунок 21 - Зависимость временных затрат от количества интегрируемых порталов

На рисунке 21 представлены итоговые показатели динамики затрат на интеграцию порталов.

«Количество и квалификация людей, требуемых для работы при грубом расчёте, можно принять для двух рассматриваемых вариантов. Между тем следует отметить, что на глобальном уровне сети корпоративных порталов вводится лишь одна роль (администратор сети), остальные роли (администратор пользовательского домена, администратор сервера доступа)

политически остаются в рамках существующих разграничений между корпоративными порталами, в случае же использования объединённого портала все существующие решения требуют переработки и внедрение в структуры объединённого портала»[34].

4.6.2. Оценка качества разграничения доступа

«Было выявлено, что эффективность системы разграничения доступа определяется через составляющие - конфиденциальность и доступность, являющиеся противоположными.

После использования методики, изложенной в диссертации, становится возможным оценить подсистему разграничения перекрёстного доступа с использованием пользовательских доменов для предложенной ранее формализованной модели.

Целевой функцией эффективности системы разграничения доступа *E* является линейной комбинацией функции доступности информации *A* и функции конфиденциальности информации *C:*»[34].

$$E = wi - A + w2 - C, (4.3)$$

«где *w* + u>2 = 1 —*весовые коэффициенты, отражающие политику разграничения доступа, в аспекте соотношения конфиденциальности и доступности информации в системе. Используемый подход описан в работе. Функции *A и L* определяются системой и конкретными характеристиками доступа субъектов к объектам»[32].

«Максимальное значение функции *E* достигающееся при использовании конкретных назначений доступа считается оптимальным. Изменение функций *A и C,* следовательно и *E* может происходить в процессе администрирования системы (добавление/удаление/изменение объектов, субъектов, прав доступа и т.д.). Исходя из этого, задачей создания средств

количественного анализа систем разграничения доступа является синтез таких функций *A и C,* которые в качестве аргументов имели бы параметры всех объектов, субъектов, и прав доступа»[32].

Обобщенная модель системы разграничения доступа 4.10 может быть представлена двудольным графом *G* = (5, O, *P).*

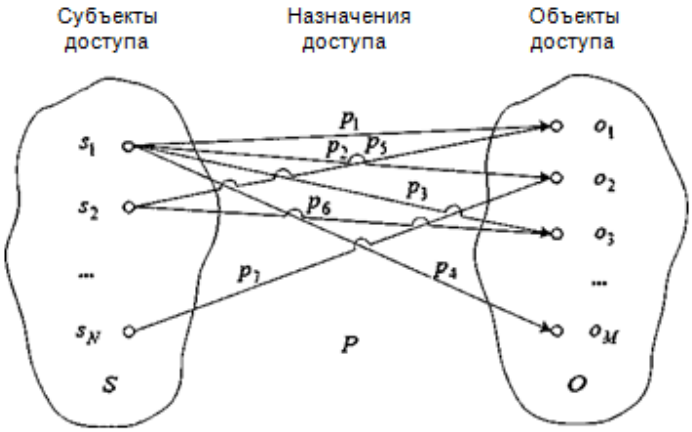


Рисунок 22 - Модель обобщенной системы разграничения доступа

На рисунке 22 представлен набор прав доступа представлен дугами графа— *P,* субъекты системы вершинами левой доли — *S* = (s_1, S_2,..., s_n), объекты доступа вершинами правой доли — *O* = (o_1, 0_2,..., o_n).

«Права доступа описываются вещественно-значимой функцией, определяющей вес соответствующей дуги графа в аспекте доступности (вес *p1)* и с точки зрения безопасности возможных действий пользователя в системе (вес *p)*»[32].

«Для субъектов доступа заданы количественные параметры значимости (вес важности s) и безопасности (вес доверия s^c_n). Для объектов доступа можно определить их вес в аспекте важности соответствующих объектов для функционирования системы и в аспекте неопасности для системы (вес o^c_n). Следовательно графовую модель можно представить совокупностью двухкомпонентного вектора весов субъектов доступа S(S_a, S_c),

двухкомпонентного вектора весов объектов доступа 0(O_a, O_c) и двухкомпонентной *n* x *m* матрицы прав доступа P(P_a, P_c)»[32].

На основе расчетов, можно сделать вывод, что примененная и использованная подсистемы разграничения перекрёстного доступа к ИР корпоративных порталов ООО «ИЦ АЙ-ТЕКО» эффективна, исходя из того, что полученный коэффициент достаточно близок к 1.

4.7. Модель функционирование сети порталов на макроуровне

«Приведённую ранее формализованную модель можно использовать для статического анализа сети, устанавливая важные для её функционирования топологические характеристики»[1].

«Также важны такие показатели функционирования сети, как уровень согласованности (вероятность отказа в обслуживании привилегированному пользователю), отказоустойчивость, максимально допустимая нагрузка и др.»[3].

«Важно обратить внимание на пропускную способность каналов связи, скорость передачи данных по каналам, время отклика серверов, способность серверов выдерживать высокую нагрузку и др»[33].

«Для узлов, соответствующих серверам различных типов, важнейшими будут следующие характеристики:

– время обработки запроса (данная величина является случайной, причём для управляющих серверов доступа время обработки запроса зависит от времени отклика сервера, которому фактически адресован запрос);

– вероятность отказа (данная величина является случайной и в общем случае коррелирует с параметрами *a* и b)»[5].

«Статическая взаимосвязь обусловлена тем, что наблюдается резкое падение скорости обработки запросов при достижении некоторого порога количества одновременно обрабатываемых запросов для реальных серверов, причём этот порог зачастую зависит от ПО, установленного на сервере.

Важен тот факт, что при снижении количества запросов ниже порога время обработки запроса не возвращается к номинальному значению, получается данный эффект устойчив. Это приводит к необходимости некоторого динамического изменяющегося параметра *beta,* который хотя и зависит от характеристик сервера *a,* но эта зависимость неочевидна и нет никакой возможности с достаточной точностью определить её в общем виде (хотя бы потому, что параметр *a* является составным и описывает совокупное влияние множества характеристик сервера)»[10]. «Для узлов-источников очевидно необходимой характеристикой является период между двумя последовательно посылаемыми запросами. Период является случайной величиной»[32]. «В модели возникают следующие основные события: возникновение запроса; возникновение ответа на запрос; остановка сервера (в результате сбоя, планового обслуживания, замены и т. п.); выход сервера из строя; возобновление работы сервера; приход уведомления об изменениях; авторизация пользователя; завершение сессии пользователя. По итогам экспериментов доступна возможность в оценке времени доступа к различным корпоративным ресурсам сети, вероятность отказа в обслуживании пользователю, надёжность отдельных участков сети и пр. Однако следует отметить, что приведённая имитационная модель способна с достаточной точностью описать функционирование сети порталов только на макроуровне»[33].

«Её не следует использовать для оценки таких параметров, как востребованность и фактическая доступность отдельных ресурсов сети, активность различных ролей пользователей, оптимальность распределения ресурсов по доменам и т. п., для оценки таких параметров следует использовать более специализированные модели. Целью также может являться имитационного моделирования подсистемы разграничения доступа в сети корпоративных порталов ООО «ИЦ АЙ-ТЕКО» эффективности разграничения доступа, при использовании предложенной подсистемы (выражающееся в сокращении ошибок первого и или второго рода).

Рассматриваемые процессы идентификации, аутентификации и авторизации субъектов могут быть представлены в виде системы массового обслуживания»[33].

«С учётом этого, а так же характера поступления заявок и распределения запросов от субъектов по сети корпоративных порталов в качестве критерия оценки эффективности функционирования рассматриваемой системы была выбрана пара распределений случайных величин - средние значения количества ошибок первого и второго рода. При этом за единицу модельного времени была выбрана величина, позволяющая передавать данные запросов субъектов по каналу за единицу модельного времени»[30].

Когда выполняется программа, осуществляется моделирование 1 млн. единиц в соответствии с модельным временем[11]. На протяжении этого времени осуществляется формирование запросов в соответствии с тем, что они случайно принадлежат порталу по равновероятному распределению.

Выводы к главе 4

В данной главе спроектирована архитектура того, как подсистема реализуется в соответствии с тем, что разделяется перекрестный доступ в соответствии с ИР корпоративного портала рассматриваемой в текущей работе организации, когда разделяются программные компоненты в соответствии с устройствами.

Осуществляется предложение технического решения для того, чтобы использовать фронтальный We-сервер, которые является обратным прокси-сервером, чтобы распределить HTTP-трафик в соответствии с ресурсами порталов, которые контролируются посредство одного сервера доступа.

Осуществляется использование правил того, как разграничить перекрестный доступ в соответствии с ИР корпоративными порталами рассматриваемой в текущей работе организации, предложение

организационных и эффективных технических решений, чтобы реализовать поставленную задачу.

Чтобы организовать взаимодействие между компонентами, были проанализированы потоки в соответствии с рассматриваемыми компонентами, а также характер того, как осуществляется информационный контакт. В соответствии с проведенным анализом определяется целесообразность использования разнообразны потоков информации.

В качестве исходных данных для того, чтобы оценить качество того, как разграничивается перекрестный доступ в соответствии с корпоративным порталом рассматриваемой в текущей работе организации, выступают пользователи, домены, роли пользователей и доменов, процедуры с их функциональными модулями. Также стоит отметить введение категорий ИР, которые также были классифицированы в соответствии с конфиденциальностью, целостностью и доступностью. Также стоит отметить, что в соответствии с огромным количеством назначений доступа с расширенными пользовательскими правами, осуществляется расширение доступности системы.

Была оценена разработанная подсистема в соответствии с тем, как разграничивается перекрестный доступ в соответствии с корпоративными порталами рассматриваемой в текущей работе организации. Коэффициент эффективности находится на отметке порядка 0,78, в соответствии с которым подтверждается то, что реализованные технические решения обладают достаточно высокой эффективностью.

Моделирование проводится для того, чтобы выявить эффективность в соответствии с разделением доступа, когда применяется предложенная подсистема. Когда выполняется программа, осуществляется моделирование 1 млн. единиц в соответствии с модельным временем. На протяжении этого времени осуществляется формирование запросов в соответствии с тем, что они случайно принадлежат порталу по равновероятному распределению.

Заключение

Поставленная задача научного характера о разработке методов и приёмов управления перекрёстным доступом в организационно-научно-технических распределённых комплексов ООО «ИЦ АЙ-ТЕКО», функциональных задач и объектов управления и их алгоритмизации, решена.

Характерной чертой деятельности ООО «ИЦ АЙ-ТЕКО» является следующие способы интеграции:

- вертикальная интеграция, которая представляет собой передачу данных снизу вверх по схеме и ликвидацию различий в справочной информации.

- горизонтальная интеграция дозволяет разным прибавлениям, задачам, а также юзерам использовать всю свою (и разрешенную в строгом соответствии с политикой разделенья доступа) информацию, вычислительные массивности, программы.

Средства администрирования и управления контентом корпоративного портала, ориентированы на исполненье стандартных функций управления ИС корпоративного уровня, отличающихся от информационно-аналитических систем, созданных для автоматизации производственной инициативности, поскольку дают обеспечение управление бизнес - логикой и имеют в личном составе визуальную среду разработки, которая дает возможность использовать дополнения, без особых знаний, навыков и умений программиста.

При авторизации пользователя фиксируется IP-адрес компьютера, с которого был осуществлен вход. Затем, при последующих запросах или авторизации в системе проходит проверка этого IP-адреса.

Поставленную задачу необходимо решать основываться на разработке сети веб-интерфейсов для доступа сотрудников к корпоративным данным, в которой происходит интеграция ИР организации ООО «ИЦ АЙ-ТЕКО».

Разработанная система должна быть центром управления, классифицирующим ИР, управляющим перекрёстным доступом в рамках сети.

Также осуществляется разработка и предложение модели управления доступом в соответствии с корпоративными порталами.

Приняты за фундамент правила доступа к информационным ресурсам.

Было установлено, уровень привилегий, представленный в виде индикатора и определяющий к каким ИР юзер имеет доступ в рамках домена.

Уровень привилегий определяется уровнем конфиденциальности присвоенной пользователю.

Выявлено, что существует возможность вносить дополнительные ограничения для достижения высокого уровня гибкости управления, например:

– Продолжительность сеанса пользователя,

– Тип соединения между компонентами и др.

Была предложена система доменов, существующих в иерархии, пользователей и использование групп, внутри которых пользователи обладают равноценными правами.

Кроме того, было предложено использовать систему индикаторов для ресурсов, определяющих возможность осуществить какие-либо операции.

Было выявлено, что существует возможность не учитывая подразделения, к которым принадлежит пользователь, объединить пользователей по уровню.

Для каждого прецедента характерно выступать в качестве законченного потока явлений в соответствии с подсистемой, где разграничивается доступ в соответствии с корпоративными порталами рассматриваемой в текущей работе организации.

Для преодоления препятствий в работе системы, осуществляется структурирование объектных моделей системы так, что для каждой характерно выступать в качестве отдельного фактора ее применения.

В соответствии с применяемой методикой стоит отметить, что каждый фактор обладает соответствием в соответствии с одним прецедентом системы в целом, он описан только теми объектами, который выступают в качестве участника такого прецедента.

Применение объекта осуществляется в соответствии с разнообразными прецедентами.

Когда исследуется предложенная методика, осуществляется определение следующих практических ограничений:

– для корпоративного портала характерно наличие системы управления контентом;

– осуществляется учет физического подключение сервера, с помощью которого обслуживается корпоративный портал и имеется возможность к тому, чтобы подключить сервер доступа;

– возможно временно отказывать в соответствии с обслуживанием на иерархии провайдера.

Также осуществляется представление фундаментальных участников процесса, в соответствии с которым формируется сеть в соответствии с корпоративными порталами и их ключевыми задачами:

– владельцы порталов сети формируют структуру портала, контролируют функционирование узла системы доступа и обращения в соответствии со связанными друг с другом порталами, регулируют работу учетных записей пользователей;

– центр управления сетью корпоративных порталов ООО «ИЦ АЙ-ТЕКО» осуществляется управление и контролирует доменные группы, делегирует администраторские полномочия, контролирует доступ в соответствии с группами домена, контролирует то, как функционирует вся сеть, а также реплицирует данные;

– пользователи сети получают доступ в соответствии с открытыми разделами портала и авторизованный доступ в соответствии с закрытыми разделами корпоративного портала.

Проведена разработка алгоритмов, в соответствии с каждой стадией рассматриваемого способа.

В данной главе спроектирована архитектура того, как подсистема реализуется в соответствии с тем, что разделяется перекрестный доступ в соответствии с ИР корпоративного портала рассматриваемой в текущей работе организации, когда разделяются программные компоненты в соответствии с устройствами.

Осуществляется предложение технического решения для того, чтобы использовать фронтальный Web-сервер, которые является обратным прокси-сервером, чтобы распределить HTTP-трафик в соответствии с ресурсами порталов, которые контролируются посредство одного сервера доступа.

Осуществляется использование правил того, как разграничить перекрестный доступ в соответствии с ИР корпоративными порталами рассматриваемой в текущей работе организации, предложение организационных и эффективных технических решений, чтобы реализовать поставленную задачу.

Чтобы организовать взаимодействие между компонентами, были проанализированы потоки в соответствии с рассматриваемыми компонентами, а также характер того, как осуществляется информационный контакт. В соответствии с проведенным анализом определяется целесообразность использования разнообразны потоков информации.

В качестве исходных данных для того, чтобы оценить качество того, как разграничивается перекрестный доступ в соответствии с корпоративным порталом рассматриваемой в текущей работе организации, выступают пользователи, домены, роли пользователей и доменов, процедуры с их функциональными модулями.

Также стоит отметить введение категорий ИР, которые также были классифицированы в соответствии с конфиденциальностью, целостностью и доступностью.

Также стоит отметить, что в соответствии с огромным количеством назначений доступа с расширенными пользовательскими правами, осуществляется расширение доступности системы.

Была оценена разработанная подсистема в соответствии с тем, как разграничивается перекрестный доступ в соответствии с корпоративными порталами рассматриваемой в текущей работе организации. Коэффициент эффективности находится на отметке порядка 0,78, в соответствии с которым подтверждается то, что реализованные технические решения обладают достаточно высокой эффективностью.

Моделирование проводится для того, чтобы выявить эффективность в соответствии с разделением доступа, когда применяется предложенная подсистема.

Когда выполняется программа, осуществляется моделирование 1 млн. единиц в соответствии с модельным временем. На протяжении этого времени осуществляется формирование запросов в соответствии с тем, что они случайно принадлежат порталу по равновероятному распределению.

Список используемой литературы и используемых источников

1. Асташенко, В .Г. Архитектура и программное обеспечение пространственно-распределённых вычислительных систем [Текст] / Виктор Гаврилович Асташенко, М. Г. Курносов, С. Н. Мамойленко, А. Ю. Поляков // Вестник ГОУ ВПО «СибГУТИ». - 2010.- № 2.— С. 112-122.

2. Воеводин, В. В. Параллельные вычисления [Текст] / В. В. Воеводин, Вл. В. Воеводин. - СПб. : БХВ-Петербург, 2002. - 608 с. - ISBN: 5-94157-160-7.

3. ГОСТ Р ИСО/МЭК 14764-2002. Информационная технология. Сопровождение программных средств [Текст]. — М. : Изд-во стандартов, 2002. — 32 с

4. Гостехкомиссия России. Руководящий документ: Защита от несанкционированного доступа к информации. Термины и определения [Текст].— М. : ГТК РФ, 1992. — 13 с.

5. Девянин, П. Н. Анализ безопасности управления доступом и информационными потоками в компьютерных системных [Текст] / Петр Николаевич Девянин. — М.: Радио и связь, 2016. - 176 с.

6. Девянин, П. Н. Модели безопасности компьютерных систем: Учебное пособие для студ. высш. учеб. заведений [Текст] / Петр Николаевич Девянин. — М. : Издательский центр «Академия», 2015. - 144 с.

7. Демидов, А. В. Автоматизация разграничения перекрёстного доступа к информационным ресурсам корпоративных порталов : на примере газотранспортных предприятий : диссертация ... кандидата технических наук : 05.13.06 / Демидов Александр Владимирович; [Место защиты: Гос. ун-т - учебно-научно-произв. комплекс]. - Орел, 2013. - 151 с. : ил.

8. Демидов, А. В. Анализ и выбор протоколов взаимодействия распределенных компонентов системы управления информационным обменом сети корпоративных порталов [Текст] / Александр Владимирович

Демидов, Сергей Александрович Лазарев // Информационные системы и технологии (ИСиТ-2018). — Т. 1., 2018. — С. 180-185.

9. Демидов, А. В. Концепция построения системы управления информационным обменом сети корпоративных порталов [Текст] / Александр Владимирович Демидов, Сергей Александрович Лазарев // Информационные системы и технологии. — 2018. — №4 (60).-С. 123-129.

10. Демидов, А. В. Концепция построения системы управления информационным обменом сети образовательных порталов [Текст] / Александр Владимирович Демидов, Сергей Александрович Лазарев // Информационные технологии в науке, образовании и производстве. — Т. 5. — [Б. м. : б. и.], 2017. — С. 80-86.

11. Демидов, А. В. Модель подсистемы разграничения доступа системы управления информационным обменом сети корпоративных порталов [Текст] / Александр Владимирович Демидов // Прикладная математика, управление и информатика. — Т. 1. 2016.-С 65-68.

12. Демидов, А. В. Обратный прокси-сервер в рамках системы управления информационным обменом сети web-порталов [Текст] / Александр Владимирович Демидов, Владимир Тарасович Еременко, Сергей Александрович Лазарев // Информационные системы и технологии (ИСиТ-2011).- Т. 1.- [Б. м. : б. и.], 2017.- С. 170-174.

13. Демидов, А. В. Проектирование подсистемы разграничения доступа к порталам органов государственной власти [Текст] / Александр Владимирович Демидов, Владимир Тарасович Еременко, Дмитрий Владимирович Агарков // Информационное развитие России состояние, тенденции и перспективы (региональный аспект). Сборник научных статей 2-й межрегиональной научно-практической конференции (22 апреля 2016). - [Б. м. : б. и.], 2016. - С. 5

14. Демидов, А. В. Управление информационными потоками на основе резервирования ресурсов в сетях передачи данных предприятий [Текст] / Александр Владимирович Демидов, Александр Иванович

Офицеров, Владимир Тарасович Еременко // Известия ОрелГТУ Серия «Фундаментальные и прикладные проблемы техники и технологии: информационные системы и технологии».— 2017.— № 4-2/268 (535).— С. 167-172.

15. Демурчев, Н. Г. Проектирование системы разграничения доступа автоматизированной информационной системы на основе функционально-ролевой модели на примере высшего учебного заведения [Текст] : Дисс... кандидата наук / Никита Георгиевич Демурчев ; ГОУ ВПО «Ставропольский государственный университет».— [Б. м. : б. и.], 2016.

16. Ерёменко, В. Т. Концепция обнаружения и коррекции логических ошибок в реализациях профилей протоколов безопасности [Текст] / В. Т. Ерёменко // Телекоммуникации. - 2013. - № 8. - С. 30-35.

17. Еременко, В. Т. Функциональная стандартизация протоколов информационного обмена в распределенных управляющих системах [Текст] : Дисс.. . доктора наук : 05.13.06 / Владимир Тарасович Еременко ; Орловский государственный технический университет. — Орёл : [б. и.], 2015. — 404 с.

18. Ерёменко, В. Том 3. Актуальные технико-экономические и организационные аспекты информатизации В 2-х кн.: Кн. 1. [Текст] / В.Т. Ерёменко, А.П. Фисун, В.А. Минаев. - Орёл : ОГУ, ГУ-УНПК, 2012.

19. Йордон, Э. Структурные модели в объектно-ориентированном анализе и проектировании [Текст] / Э. Йордон, К. Аргила. — М. : Лори, 1999. — 264 с. — ISBN: 5-85582-057-2.

20. Лазарев, С. А. Применение цифровых носителей идентификационной информации для управления доступом в сети корпоративных порталов [Текст] / Сергей Александрович Лазарев, Павел Павлович Силаев // Информационные системы и технологии. - 2017. - № 3 (65). - С. 114-119.

21. Ларман, К. Применение UML и шаблонов проектирования. 2-е издание [Текст] / К. Ларман. — М. : «Вильяме», 2016. — 624 с.

22. Липаев, В. В. Процессы и стандарты жизненного цикла сложных программных средств. Справочник [Текст] / В. В. Липаев. — М. : Синтег, 20106. — 608 с.

23. Липаев, В. В. Системное проектирование сложных программных средств для информационных систем [Текст] / В. В. Липаев. — М. : Синтег, 2015. — 268 с.

24. Липаев, В. В. Функциональная безопасность программных средств [Текст] / В. В. Липаев. - М. : Сиитег, 2014. — 348 с.

25. Максименко, С. В. Методы и средства технической диагностики оборудования компрессорной станции [Текст] / С. В. Максименко, Г. Н. Поляков, А. Н. Труфанов. Обзорная информ. Серия «Транспорт и подземное хранение газа». — М. : ВНИИЭга-зпром, 2016. — 66 с.

26. Мацяшек, Л. Анализ требований и проектирование систем. Разработка информационных систем с использованием UML [Текст] / Лешек Мацяшек. — М. : «Вильяме», 2010. - 432 с. - ISBN: 5-8459-0276-2.

27. Методика оптимизации структуры кампусных компонентов корпоративных сетей предприятия [Текст] / В. Т. Ерёменко, С. И. Афонин, О. В. Третьяков, СВ. Ерёменко // Известия Тульского государственного университета. Серия «Технологическая системотехника». — 2016. — № 13. — С. 13-22.

28. Многоуровневые информационно-управляющие системы реального времени для топливно-энергетического комплекса России: Монография [Текст] / Под ред. В. Е. Костюкова. — Нижний Новгород : Изд-во ННГУ им. Н. И. Лобачевского, 2017. — 243 с.

29. Моделирование процесса формирования экспертной группы по заданной тематике [Текст] / В. Т. Еременко, М. А. Сазонов, СИ. Фомин, В. А. Петров // Информационные системы и технологии. — 2015.— № 3.— С. 23-31.Таненбаум, Э. Распределенные системы. Принципы и парадигмы [Текст] / Э. Танен-баум, М. ван Стеен. - СПб. : Питер, 2013. - 880 с. - ISBN: 5-272-00053-6.

30. Теория информации и информационных процессов: Монография [Текст] / В.Т. Ерёменко, И.С. Константинов, А.В. Коськин [и др.].— Орёл : ОГУ, ОрелГТУ, 2018.— 478 с.

31. Тихонов, Д. В. Модели оценки эффективности систем информационной безопасности [Текст] : Дисс... кандидата наук / Денис Вахтангиевич Тихонов ; ГОУ ВПО «Санкт-Петербургский государственный инженерно-экономический университет». — [Б. м. : б. и.], 2016.

32. Qingcang, Y. Web based control system design and analysis [Text] / Yu Qingcang, Chen Bo, H. H. Cheng // IEEE Control Systems Magazine. - 2004. - Vol. 24, no. 3. -P. 45-57.

33. Sullivan, D. Proven Portals: Best Practices for Planning, Designing, and Developing Enterprise Portals [Text] / Dan Sullivan. — [S. 1.] : Addison-Wesley Professional, 2003. — 224 p.-ISBN: 0321125207.

34. Terra, J. C. C. Realizing the Promise of Corporate Portals: Leveraging Knowledge for Business Success [Text] / Jose Claudio Cyrineu Terra, Cindy Gordon. — [S. 1.] : Butter-worth-Heinemann, 2002. - 256 p. — ISBN: 0750675934.

35. Townsend, J. J. Building Portals, Intranets, and Corporate Web Sites Using Microsoft Servers [Text] / James J. Townsend, Dmitri Riz, Deon Schaffer. — [S. 1.] : Addison-Wesley Professional, 2004. - 544 p. - ISBN: 0321159632.

36. Yang, S. H. Requirements specification and architecture design for internet-based control systems [Text] / S. H. Yang, L. S. Tan, X. Chen // 26th Annual International Computer Software and Applications Conference. — [S. 1. : s. п.], 2002. — P. 75-80.