Product manager: Валерий Хвостенко
Дата последней редакции: 15.05.2001
Версия проекта: 01
Версия документа: 08

Функциональная спецификация

к проекту «Возвращенные Имена»
(Единый Электронный Банк Данных по репрессированным)

Содержание

Данный документ представляет развернутое описание построения и функционирования как системы в целом, так и отдельных ее частей.

В состав документа входит концептуальный, логический и физический дизайн системы, которые в совокупности дают полную картину: на каких принципах, по каким алгоритмам, как и с помощью каких средств построена и функционирует система.

КОНЦЕПТУАЛЬНЫЙ ДИЗАЙН ПРОЕКТА "ВОЗВРАЩЕННЫЕ ИМЕНА"

Описание программного комплекса

Исходя из целей проекта, условий его успешной реализации и требований, предъявляемых к функциональности и надежности системы, предлагается реализовать программный комплекс в виде:

- центрального узла, на котором реализуется вся бизнес-логика[1] и веб-интерфейсы удаленных пользователей,
- и автономной клиентской части, работающей с локальной базой данных и использующей сеансовый доступ к центральному узлу.

Условно весь комплекс можно разбить на 3 части:

- Платформенная часть
- Серверная часть
- Клиентская часть

Платформа

В качестве платформы предлагается использовать технологии и продукты компании Microsoft:

- Сетевая операционная система **Microsoft Windows 2000 Advanced Server** объединяет поддержку кластеризации при сбоях в работе приложений с интегрированной балансировкой нагрузки сети и приложений, что делает возможным выполнение масштабируемых приложений с непрерывным доступом к данным в многоуровневой среде **Windows 2000**.
- Брандмауэр **Microsoft Internet Security and Acceleration (ISA) Server,** способный защищать сеть от попыток несанкционированного доступа, отражать атаки извне, анализировать входящий и исходящий трафик с точки зрения безопасности, а также уведомлять администраторов об обнаружении подозрительной деятельности. В дополнение ко всему, **ISA Server** имеет встроенный высокоскоростной кэш информационного наполнения Web, позволяющий обеспечить высокую производительность. **ISA Server** имеет встроенную поддержку исполнения на линейках серверов для построения кластеров брандмауэров. Встроенные средства поддержки **VPN** (Virtual Private Networking – Виртуальных частных сетей, или туннелей) обеспечат высокую надежность и безопасность сеансов связи с локальными клиентами.
- Сервер баз данных **Microsoft SQL Server 2000 -** это законченное решение в области баз данных и анализа данных для быстрого создания масштабируемых приложений и хранилищ данных. В сервер **SQL Server 2000** включены: поддержка языка **XML** и протокола HTTP; средства повышения быстродействия и доступности, позволяющие распределить нагрузку и обеспечить бесперебойную работу; функции для улучшения управления и настройки, снижающие совокупную стоимость владения и обслуживания, что немаловажно в рамках данного проекта.

[1] **Примечание** «Бизнес-логика» - общепринятый термин, не имеющий отношения к какой-либо коммерческой деятельности. Он означает функциональное наполнение программы, отвечающее за выполнение основных задач обработки данных, связанных с предметной областью проекта.

- Сервер электронной почты **Microsoft Exchange 2000 Server** являющийся надежной, легкой в управлении платформой для обмена сообщениями и обеспечивающий надежную, масштабируемую и удобную в управлении инфраструктуру обмена сообщениями. Современная система хранения веб-ресурсов **Microsoft Web Storage System** позволяет объединить надежность и масштабируемость **Microsoft Exchange 2000** с доступностью и открытостью интернета.
- **Microsoft Internet Information Server 5.0** с применением технологии Active Server Pages, входящий в состав **Microsoft Windows 2000 Advanced Server**. Используется для реализации WWW-сервера, обеспечивающего доступ посетителей сайта, и реализации функционала удаленных пользователей системы с доступом через веб-интерфейс.

Серверная часть

Под серверной частью в контексте проекта подразумевается программное обеспечение, необходимое для реализации взаимодействия с удаленными клиентами. Удаленные клиенты подразделяются на 4 группы.

- Посетители;
- Администраторы;
- Поставщики информации (**тип 1);**
- Поставщики информации, (**тип 2**).

Взаимодействие с первыми тремя группами будет осуществляться посредством функционала, реализованного на базе **Microsoft Internet Information Server** с использованием ASP технологии и WEB-интерфейсов.

Посетители будут иметь доступ к базе данных только в режиме «Чтение». Администраторы и поставщики информации типа 1 имеют право на обновление базы данных в рамках своих полномочий.

Для взаимодействия с четвертой группой будет использоваться специализированное приложение-сервер, состоящее из двух модулей: коммуникационного модуля и модуля бизнес-логики. Коммуникационный модуль осуществляет прием пакетов с данными для центральной базы, прием запросов к центральной базе, аутентификацию удаленных пользователей, проверку целостности пакетов, а также отправку результатов запросов, отправку служебной информации, отправку обновлений глобальных справочников и обновлений программных модулей локального клиента с использованием транспорта, базирующегося на SMTP-протоколе, либо TCP/IP-протоколе. Модуль бизнес-логики отвечает за добавление данных, полученных от локальных клиентов в центральную базу, проверку корректности и целостности этих данных, формирование подтверждения добавления данных в базу, контроль версий глобальных справочников клиента, подготовку и отправку глобальных справочников.

Клиентская часть

Программное обеспечение клиентской части для поставщика информации 2 типа планируется как локальное приложение, состоящее из трех модулей: коммуникационного модуля, модуля бизнес-логики и модуля пользовательского интерфейса, и работающее на любой win32-совместимой платформе.

Модуль бизнес-логики отвечает за интерфейс с локальной базой данных, выполнение всех функций, связанных с модификацией данных, подготовку к отправке данных, контроль версий глобальных справочников, контроль версий локальных модулей клиентского приложения, обработку служебных сообщений центрального узла.

Коммуникационный модуль выполняет функции передачи пакетов с данными для центральной базы, отправку запросов к центральной базе, шифрование передаваемых пакетов, контроль доставки пакетов, а также прием результатов запросов, прием служебной информации, прием обновлений глобальных справочников и обновлений программных модулей локального клиента посредством транспорта, базирующегося на SMTP-протоколе, либо TCP/IP-протоколе. Пользовательский интерфейс предполагается выполнить в виде набора HTML-документов, базирующихся на HTML-коде серверной части, с целью сокращения времени разработки и **унификации интерфейса пользователя.** Таким образом, обеспечивается единая рабочая среда для различных пользователей системы, работают ли они с локальной базой или с сервером.

Программное обеспечение клиентской части для поставщика информации 1 типа планируется как набор web-интерфейсов, расположенных на WEB-сайте центрального узла. По своему интерфейсу и логике работы эти web-интерфейсы максимально приближены к интерфейсу и логике работы локального приложения.

Пользователи

Пользователи программного комплекса подразделяются на две основные группы: **группа пользователей, обеспечивающих наполнение и функционирование ЕЭБД**, и **группа пользователей, применяющих ЕЭБД в своей деятельности**, с разделением по категориям внутри групп, исходя из потребностей пользователей при взаимодействии с ЕЭБД.

1. Группа пользователей, обеспечивающих наполнение и функционирование ЕЭБД

1.1.Администратор сервера

Данная категория пользователей ожидает получить надежный, эффективный, функциональный и безопасный инструмент управления программным комплексом, его структурой и информационным наполнением.

Основными целями при разработке системы для этой группы пользователей будет создание интуитивно понятного интерфейса взаимодействия с системой, наполнение системы достаточной функциональностью для управления и динамичного развития, эффективная система безопасности и администрирования, высокая устойчивость к сбоям.

Основными требованиями можно считать, безопасность, надежность и функциональность системы.

Ограничениями могут быть: уровень подготовки администраторов.

1.2. Администратор базы данных

Данная категория пользователей ожидает получить удобный, эффективный, функциональный инструмент управления базами данных предметной области, их структурой и информационным наполнением.

Основными целями при разработке системы для этой группы пользователей будет создание интуитивно понятного интерфейса взаимодействия с системой, наполнение системы достаточной функциональностью для управления и динамичного развития, эффективная система связывания данных и управления разнородными данными.

Основными требованиями можно считать надежность и функциональность системы.

Ограничениями могут быть: уровень понимания администраторами предметной области, т.к. принятие решений нередко будет связано с тонкими особенностями поступающего материала.

1.3. Поставщик информации, тип 1

Данная категория пользователей ожидает получить удобный и функциональный инструмент для информационного наполнения ЕЭБД, публикации собственных данных для широкого круга лиц и взаимодействия с различными категориями пользователей.

Особое внимание при разработке следует уделить созданию удобного и продуманного интерфейса взаимодействия с системой. Необходимо также обеспечить целостность и достоверность вводимых данных.

Требования, которые предъявляются к проекту данной категорией пользователей: удобство пользования системой, быстрота и надежность работы, наличие развитых сервисных функций.

Ограничениями могут выступать следующие факторы: территориальная распределенность данной категории пользователей, и, как следствие, различные по качеству и скорости средства доступа в интернет, отсутствие необходимого аппаратного обеспечения, отсутствие опыта работы с современными технологиями, финансовые ограничения.

1.4. Поставщик информации, тип 2

Данная категория пользователей ожидает получить удобный и функциональный инструмент для создания и поддержания локальных баз данных со сведениями о репрессированных, возможность содействия информационному наполнению ЕЭБД, возможность публикации собственных данных для широкого круга лиц и взаимодействия с различными категориями пользователей, осуществление научной и поисковой деятельности в среде ЕЭБД.

Особое внимание при разработке следует уделить созданию надежной системы удаленного взаимодействия с ЕЭБД, гарантирующей целостность и адекватность поставляемой информации, необходим также удобный и продуманный интерфейс взаимодействия с системой, обеспечение целостности и достоверности вводимых данных,

Требования, которые предъявляются к проекту данной категорией пользователей: удобство пользования системой, быстрота и надежность работы, наличие развитых сервисных функций, нетребовательность к характеристикам линий связи.

Ограничениями могут выступать следующие факторы: отсутствие необходимого аппаратного обеспечения, отсутствие опыта работы с современными технологиями, финансовые ограничения.

2. Группа пользователей, применяющих ЕЭБД в своей деятельности

2.1. Репрессированные и их родственники

Эта категория пользователей надеется бесплатно и быстро, в удобном и доступном месте получить точную информацию о родных, ставших жертвами репрессий, об источниках этой информации и узнать о социальных льготах, на которые они могут рассчитывать.

Основная цель - сведение воедино всей информации о репрессированных, создание информационных центров, где каждый пользователь может получить такую информацию с использованием интернета или другим приемлемым способом (по телефону или письменно, по специально разработанной форме).

Требования - бесплатность, быстрота, доступность, точность информации.

Ограничения - пользователи живут в самых разных местах, в том числе и за границей. Лишь у немногих есть современные средства связи, большинство не владеет современными технологиями, облегчающими получение информации (интернет). Письменная переписка требует дополнительного финансирования и времени.

2.2. Ученые-исследователи

Эта категория пользователей ожидает быстрого получения точной, качественной, достоверной и, по возможности, полной информации по всей истории репрессий. Особенно интересует источник информации и объективность полученных сведений, а также доступ к справочникам по теме исследований. В отличие от прочих пользователей, для исследователей более важны выборки и действия над ними, чем конкретные персоналии. Им необходимы средства статистической обработки данных и наглядного представления результатов со средствами выполнения запросов и выборок по полной базе.

Приоритеты этой группы: полнота, достоверность, четкость структуры представляемой информации, а также перевод в электронный вид информации об источниках по теме репрессий, самого текста источников, различных справочных материалов, литературы, данных о персоналиях.

Основными требованиями этой категории пользователей будет дешевизна использования системы, быстрота, доступность, точность, проверенность информации.

Ограничения связаны с наличием времени, необходимого для обучения и работы с системой, деньгами, которые необходимо затратить на обеспечение доступа к системе, отсутствием доступа к интернету и неумением пользоваться ПК.

Основной фактор, влияющий на успех проекта в данной категории: неготовность идти на большие денежные затраты, потеря интереса при сомнении в объективности информации или трудности в ее получении.

2.3. Служащие государственных учреждений

Эта категория пользователей надеется быстро получить точную информацию о репрессированных и об источниках этой информации.

Требования - доступность, точность информации, подтвержденность ее официальными документами.

Специфика заключается в том, чтобы выделить среди всего объема информации официально подтвержденную, а также получить ссылки на официальные источники этой информации.

2.4. Прочие посетители.

Эта категория пользователей ожидает качественную, интересную и полную информацию по истории репрессий. Им необходимы средства выполнения простейших запросов.

Приоритетом в этой группе является доступность информации.

Основными требованиями этой категории пользователей будет дешевизна использования системы, быстрота, доступность информации.

Ограничения связаны с наличием времени, необходимого для обучения и работы с системой, деньгами, которые необходимо затратить на обеспечение доступа к системе, отсутствием доступа к интернету или неумением пользоваться ПК.

Основной фактор, влияющий на успех проекта в данной категории - неготовность к денежным затратам, необходимым для доступа к системе, отсутствие интереса к предоставляемой информации.

Сценарии работы пользователей.

1. Группа пользователей, обеспечивающих наполнение и функционирование ЕЭБД

1.1. Администратор системы.

Осуществляет удаленный доступ к информации, расположенной на WWW-сервере Центрального Узла через интернет при помощи браузера Microsoft Internet Explorer 4.x-5.x. Для администратора реализован закрытый функционал, размещенный на www-страницах, позволяющий полностью контролировать и управлять всем программным комплексом. Администратор имеет полный доступ. Осуществляет делегирование и разграничение прав. Отвечает за создание, изменение, формирование структуры WEB-сервера. Контролирует функционирование и поддерживает работоспособность комплекса в целом.

1.2. Администратор базы данных

Осуществляет администрирование баз данных, расположенных на сервере Центрального Узла через интернет при помощи браузера Microsoft Internet Explorer 4.x-5.x или локально с использованием специализированных приложений и средств управления базами данных. Для администратора баз данных реализован закрытый функционал, позволяющий полностью управлять базами данных. Доступ – полный. Создание, удаление, изменение баз данных. Прием и обработка данных из локальных приложений, увязка.

1.3. Поставщик информации типа 1.

Осуществляет ввод, редактирование и удаление своей и только своей информации непосредственно в ЦБД через интернет при помощи браузера Microsoft Internet Explorer 4.x-5.x. Для него реализован функционал в виде набора www-страниц, расположенных на www-сервере Центрального Узла. Доступ к общим данным он осуществляет как привилегированный пользователь. Для работы Поставщика необходим сеансовый, или по выделенному каналу, доступ в интернет.

1.4. Поставщик информации типа 2.

Осуществляет ввод, редактирование и удаление информации через локальное приложение в своей локальной базе данных. Обмен данными с ЦБД происходит через интернет в сеансовом режиме. Локальное приложение и локальная база данных разрабатываются под операционные системы Windows 95/98/NT 4.0/2000.

2. Группа пользователей, применяющих ЕЭБД в своей деятельности

2.1. Репрессированные и их родственники

Пользователи этой категорий осуществляют удаленный доступ к информации, расположенной на WWW-сервере Центрального Узла, через интернет при помощи браузера Microsoft Internet Explorer 4.x-5.x. Для этих пользователей реализован функционал посетителя сайта (поиск человека по установочным данным, просмотр списка по начальным буквам, получение стандартной справки, ссылки на архив и т.п.) и открыта общедоступная информация.

2.2. Ученые-исследователи

Пользователи этой категорий осуществляют удаленный доступ к информации, расположенной на WWW-сервере Центрального Узла, через интернет при помощи браузера Microsoft Internet Explorer 4.x-5.x. Для этих пользователей реализуется функционал ученого-исследователя: доступ к другим полям, помимо установленных по умолчанию для обыкновенного посетителя; возможность выполнения сложных комбинированных запросов; получение статистической информации и инструменты для ее анализа, обработки и представления виде таблиц, графиков, гистограмм и т.п.; возможность экспорта результатов запроса и их представлений в другие системы и форматы.

2.3. Служащие государственных учреждений

Пользователи этой категорий осуществляют удаленный доступ к информации, расположенной на WWW-сервере Центрального Узла, через интернет при помощи браузера Microsoft Internet Explorer 4.x-5.x. Для этих пользователей реализован функционал посетителя сайта (поиск человека по установочным данным, просмотр списка по начальным буквам, получение

стандартной справки, ссылки на архив и т.п.) и открыта общедоступная информация, а также, в соответствии с регламентом и правами, предоставляется доступ к закрытым разделам базы, доступ к правовым и законодательным материалам, расширенной информации по источникам.

2.4. Прочие посетители.

Пользователи этой категорий осуществляют удаленный доступ к информации, расположенной на WWW-сервере Центрального Узла, через интернет при помощи браузера Microsoft Internet Explorer 4.x-5.x. Для этих пользователей реализован функционал посетителя сайта (поиск человека по установочным данным, просмотр списка по начальным буквам, получение стандартной справки, ссылки на архив и т.п.) и открыта общедоступная информация.

Матрица рисков (Risk matrix)

Важность	Воздействие	Описание	План устранения
Высокая	Высокое	Смена политической обстановки	Зеркалирование сервера в странах с устойчивой политической системой
Высокая	Высокое	Природные и техногенные катаклизмы	Зеркалирование сервера в разных географических точках
Высокая	Среднее	Отказ в государственной поддержке проекта	Использование имеющихся массивов данных, собранных общественными организациями.
Высокая	Высокое	Прекращение финансирования проекта	Организационные и технические мероприятия по «замораживанию» системы и сохранению информации для дальнейшего использования.
Высокая	Высокое	Разрушение базы данных вследствие атак, проведенных по интернету	Организация резервного копирования данных, репликация базы данных, создание системы защиты от несанкционированного вторжения.
Высокая	Высокое	Слишком длинный срок разработки	Использование принципа версионности
Высокая	Высокое	Нестабильность работы сервера	Тщательный контроль оборудования. Грамотная настройка программного обеспечения. Организационные и технические мероприятия по постоянному отслеживанию состояния сервера.
Средняя	Среднее	Чрезмерная сложность системы для пользователя	Разделение доступа по уровням сложности

ЛОГИЧЕСКИЙ ДИЗАЙН

Модули системы

Описание структурных элементов

A. Кластер на базе Microsoft Windows 2000 Advanced Server (см приложение).
B. Почтовая система на базе Microsoft Exchange 2000 Server.
C. Центральная база данных на Microsoft SQL 2000 Server для хранения всех данных в рамка проекта.
D. Серверная часть программного обеспечения, обеспечивающая функционирование центрального узла, взаимодействие с удаленными клиентами и обработку данных, поступающих на центральный узел.
E. Программное обеспечение удаленного клиента системы с локальной базой данных.
F. WWW-сервер на базе Microsoft Internet Information Server для организации доступа посетителей к ресурсам сайта и реализации функционала пользователей системы работающих с центральным узлом через интернет, а также выполнения задач администрирования.
G. WEB-интерфейс и функционал посетителя сайта.
H. WEB-интерфейс и функционал поставщика информации второго типа.
I. WEB-интерфейс и функционал администратора системы.
J. Удаленные клиенты системы с доступом через интернет.
K. Программный файрвол/фильтр пакетов на базе Microsoft ISA Server.

Описание информационных потоков.

Нумерация потоков соответствует рис 1.

Поток	Описание
1.	Данные пользователя поступают в модуль бизнес-логики, либо данные из модуля бизнес-логики передаются пользователю.
2.	Данные пользователя помещаются в локальную базу, из локальной базы происходит выборка данных для отправки в ЕЭБД, а также выборка данных, необходимых пользователю.
3.	Подготовленные к отправке новые или измененные данные передаются в коммуникационный модуль, забираются данные, принятые коммуникационным модулем из центрального узла.
4.	Подготовленные данные отправляются по SMTP-протоколу на почтовый сервер центрального узла, принимается подтверждение доставки и служебная информация (новости, обновления глобальных справочников и т.д.) от центрального узла.
5.	Подготовленные данные отправляются по TCP/IP протоколу на коммуникационный сервер центрального узла, принимается подтверждение доставки и служебная информация (новости, обновления глобальных справочников и т.д.) от центрального узла
6.	Принятые данные передаются серверу бизнес-логики, подготовленные к отправке сервером бизнес-логики данные принимаются к отправке
7.	Очереди пакетов и служебная информация сохраняется на сервере баз данных или извлекается для отправки
8.	Данные, поступающие от сервера бизнес-логики, сохраняются в базе данных; данные из базы передаются серверу бизнес-логики.
9.	Информация, получаемая IIS из пользовательских сессий сохраняется в базе данных, из базы данных выбирается информация, необходимая для поддержания функционирования веб-сервера и функционала посетителей.
10.	Обмен информацией посетителя с Веб-Сервером через www-страницы
11.	Обмен информацией поставщика типа 1 с Веб-Сервером через www-страницы
12.	Обмен информацией администратора с Веб-Сервером через www-страницы
13.	Взаимодействие посетителя сайта с Веб-Сервером через www-страницы для просмотра и поиска информации.
14.	Взаимодействие поставщика информации типа 1 с Веб-Сервером через www-страницы для размещения и управления информацией.
15.	Взаимодействие администратора с Веб-Сервером через www-страницы для управления программным комплексом.

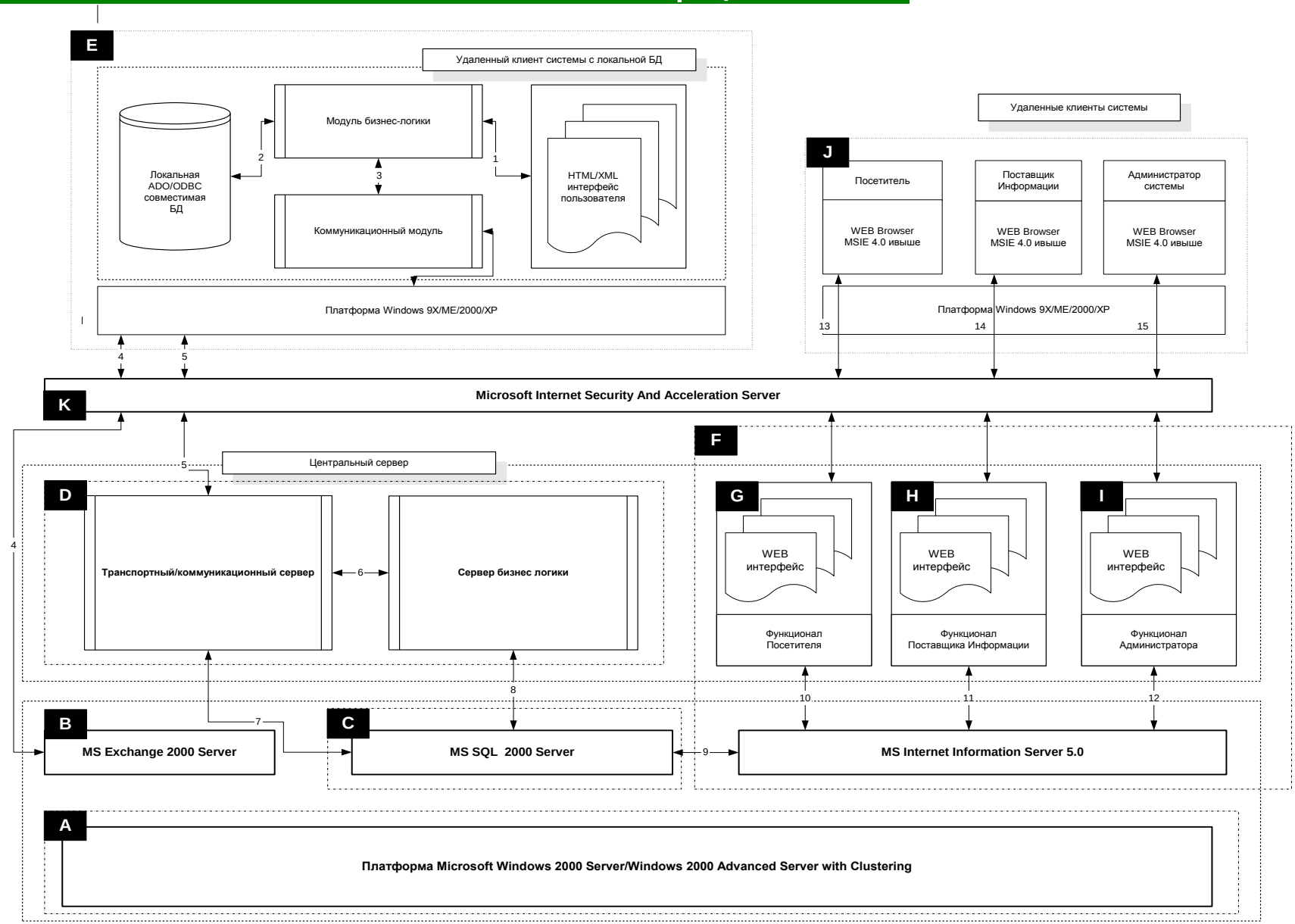


Рис 1. Схема Программного Комплекса

Описание клиентского приложения

A. Локальная база данных

A.0. Часть локальной базы в формате Microsoft Access, в которой хранятся данные предметной области (локальные справочники, глобальные справочники, документы, записи о репрессированных, и т.п.)

A.1. Часть локальной базы в формате Microsoft Access, в которой хранятся данные, необходимые для функционирования локального клиента (конфигурации клиента, параметры настроек связи, служебные сообщения от ЕЭБД, данные о версиях справочников, очереди данных для отправки, списки соответствий данных локальных и глобальных справочников, и т.п.)

B. Модуль бизнес-логики

B.0. Интерфейс к БД. Модуль, обеспечивающий прямое взаимодействие с локальной БД в формате Microsoft Access, минуя системные ODBC драйвера.

B.1. Синхронизация локальных глобальных справочников с глобальными справочниками ЕЭБД.

B.2. **О**бновление локальных данных в соответствии с изменениями в локальных и глобальных справочниках.

B.3. Формирование пакетов с новыми или измененными данными для передачи в ЕЭБД, учет переданных данных, проверка гарантированной доставки пакетов.

B.4. Формирование запросов к удаленной БД, подготовка к отправке запросов, интерпретация результатов запросов, сохранение результатов запросов в локальной БД. Удаление данных этого поставщика из глобальной БД.

B.5. Обеспечение функционирования пользовательского интерфейса, пользовательских настроек и т.д.

B.6. Реализация функционала для работы с локальной БД. Выполнение всех функций связанных с добавлением и модификацией данных в локальной БД.

B.7. Выполнение обновления программных модулей локального клиента.

B.8. Шифрование исходящих данных, дешифрование входящих данных.

C. Коммуникационный модуль

C.0. Модуль аутентификации пользователя и сервера, создающий защищенное соединение

C.1. Выполняет функции проверки целостности принимаемых пакетов, и формирование кода проверки целостности для отправляемых пакетов.

C.2. Транспортный функционал среды передачи данных. Выполняет передачу и прием данных по SMTP или TCP/IP протоколу.

D. Интерфейс пользователя

D.0. Главный интерфейс программы, предоставляющий доступ ко всему функционалу локального клиента.

D.1. Интерфейс пользователя, обеспечивающий доступ к функционалу выполнения запросов и работы с результатами запросов к локальной базе.

D.2. Интерфейс, обеспечивающий доступ к изменению настроек и параметров функционирования системы.

D.3. Интерфейс, обеспечивающий доступ к функционалу ввода и редактирования данных в локальной базе.

D.4. Интерфейс пользователя, обеспечивающий доступ к функционалу выполнения запросов к ЕЭБД и работы с результатами запросов.

D.5. Интерфейс, обеспечивающий доступ к функционалу формирования данных для отправки и контроля процесса отправки.

D.6. Интерфейс, обеспечивающий доступ к функционалу служебного взаимодействия с ЕЭБД.

Схема клиентского приложения изображена на рис. 2

Логическая схема взаимодействия клиентского приложения и ЕЭБД изображена на рис. 3

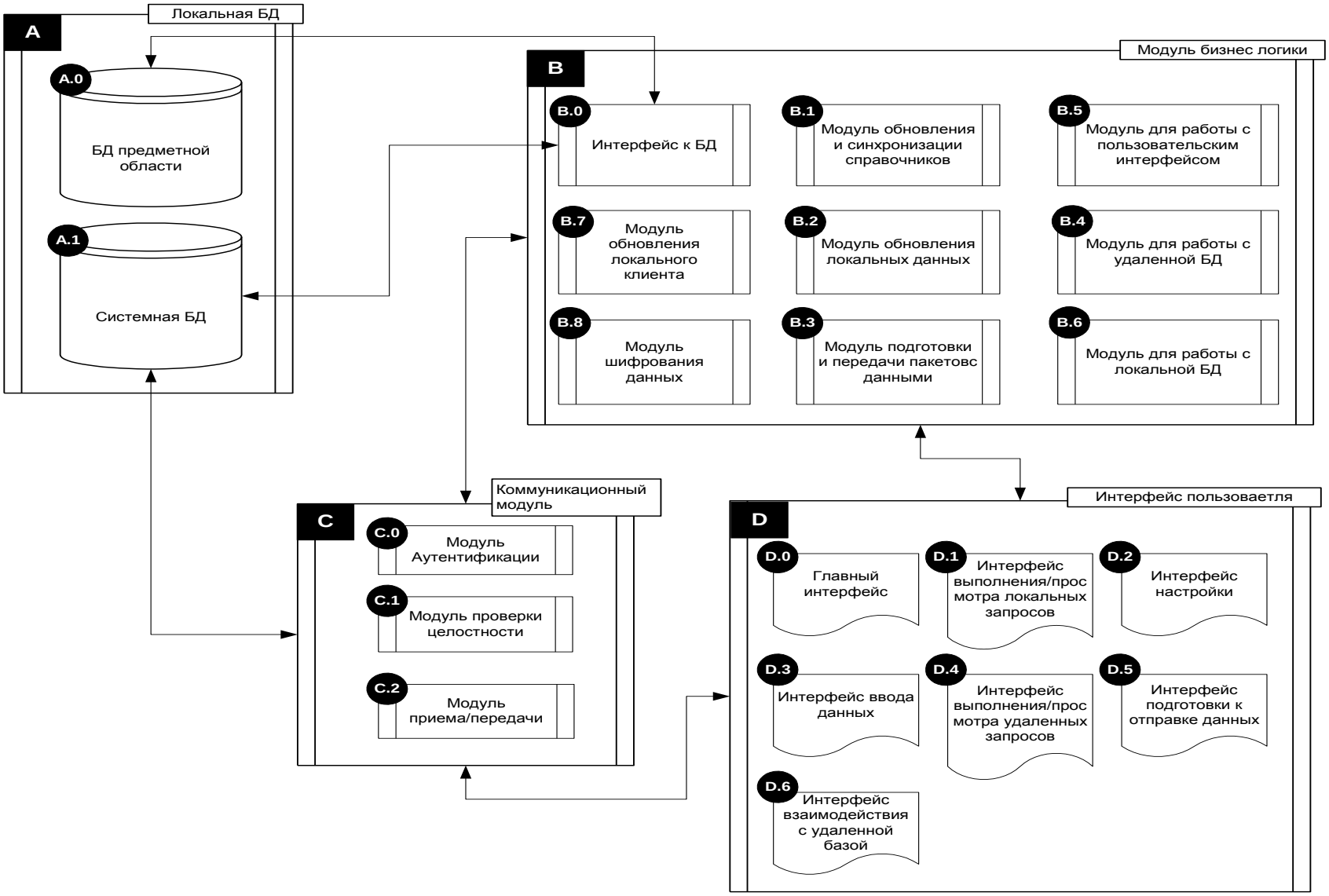
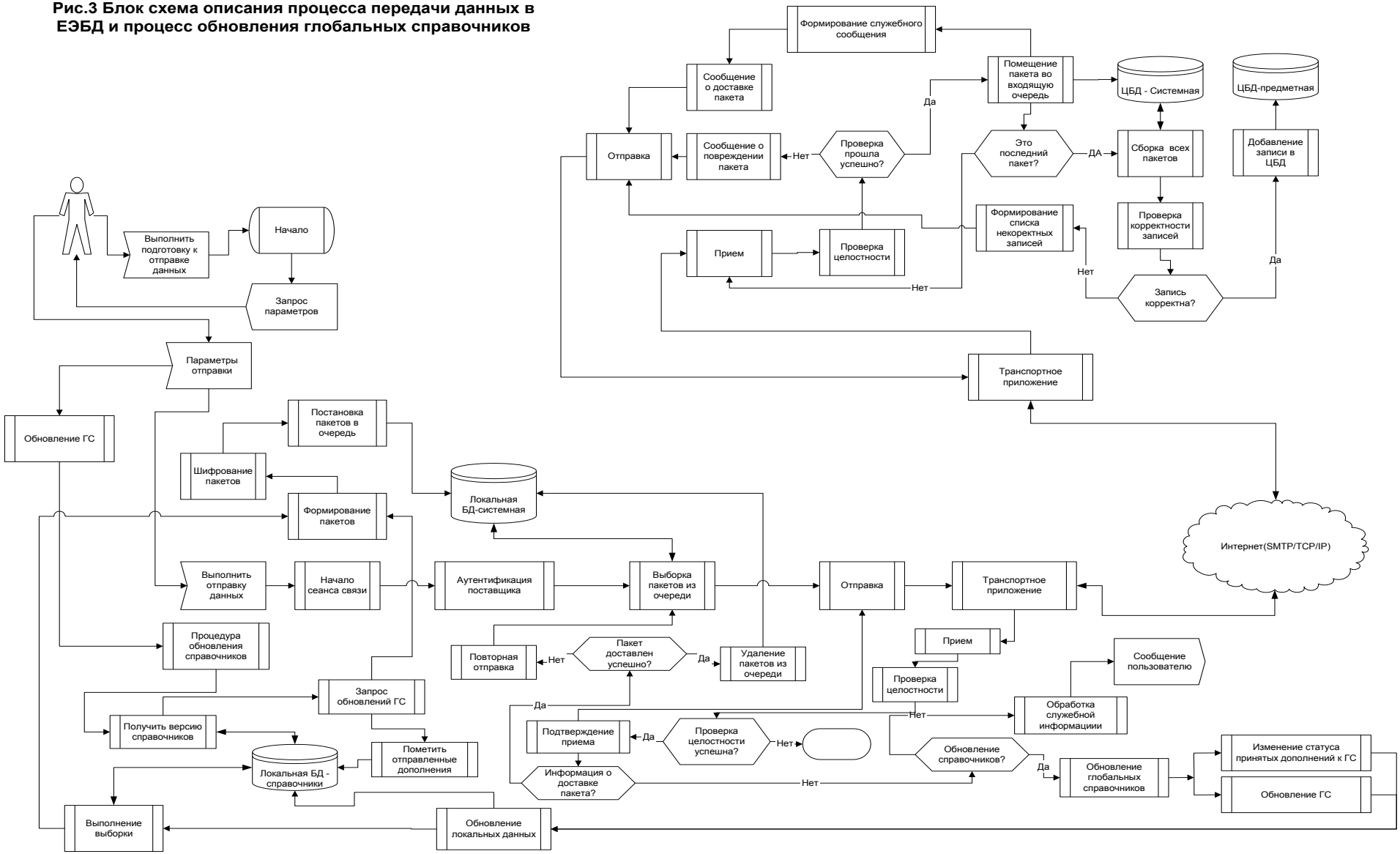


Рис.2 Схема клиентского приложения

Рис.3 Блок схема описания процесса передачи данных в ЕЭБД и процесс обновления глобальных справочников



Логическая схема взаимодействия ЕЭБД и пользователя

При входе на сайт определяется тип пользователя и, в зависимости от типа, предлагается набор возможностей и/или запрашиваются дополнительные сведения. Например, если пользователь идентифицировал себя как исследователя, у него дополнительно спрашивается пароль. Если он идентифицировал себя как родственник репрессированного, ему предлагается простая поисковая форма, и т.д.

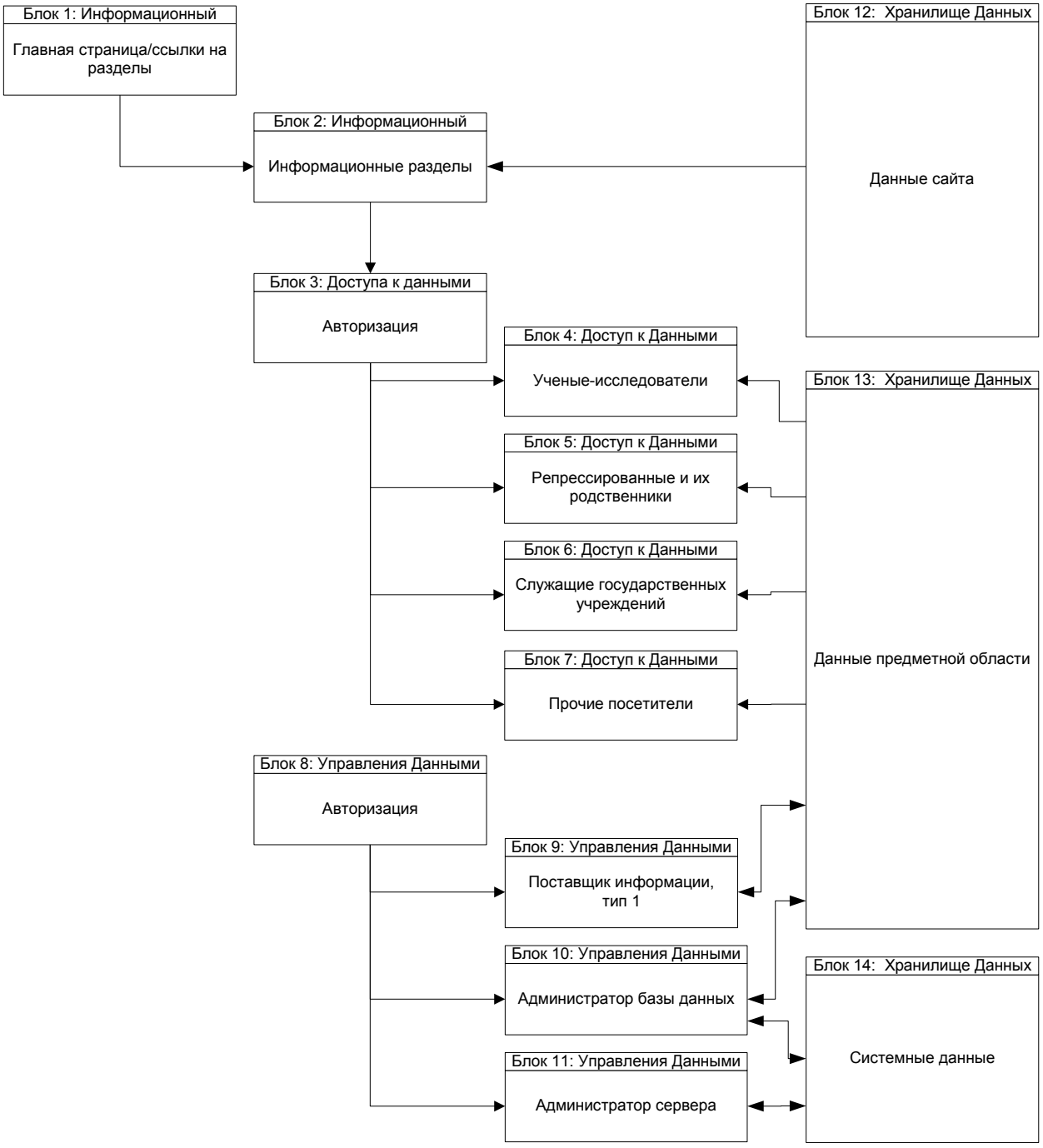


Рис.4 Логическая схема взаимодействия ЕЭБД и пользователя

Базы данных

Типы баз данных системы

Базы данных предметной области
Системные базы данных

Базы данных предметной области

Основные сущности
(Список сущностей будет пополняться)

Участник проекта
Определение: Общественная, государственная или иная организация или группа, поставляющая в Банк информацию о репрессированных по согласованному стандарту.

Репрессированный
Определение: Лицо, подвергнувшееся необоснованной судебной или внесудебной репрессии на территории советского государства в период советской власти.

Репрессия
Определение: Единичный акт судебного или внесудебного решения по отношению к репрессированному.

Заключение
Определение: Предварительное заключение в период следствия или отбывание наказания в лагере/тюрьме.

Ссылка
Определение: Пребывание в ссылке по приговору или в результате внесудебного решения.

Документ
Определение: Тип источника информации о репрессированном. Бумажный документ из официального (или иного) структурированного архива.

Публикация
Определение: Тип источника информации о репрессированном. Печатный материал, опубликованный в официальном (или ином) издании.

Сообщение
Определение: Тип источника информации о репрессированном. Сообщение другого репрессированного или не репрессированной персоны в письменном (или ином) виде.

Персона
Определение: Лицо, имеющее непосредственное отношение к репрессированному и само не являющееся репрессированным.

Сотрудник
Определение: Сотрудник репрессивных органов (в т.ч. следователь по делу), имеющий непосредственное отношение к репрессированному.

Логический дизайн
(Приведено описание некоторых таблиц базы. Структура таблиц будет уточняться.)

Biography\Биография (вариант Repressived \ Репрессированный)

Эта таблица хранит основные биографические сведения о репрессированном и является главной таблицей в схеме базы данных.

	Имя поля	Русское название	Тип поля	Комментарий
1.	Rpr_id	Код репрессированного	Счетчик	Уникальный идентификатор в базе участника
2.	Name	ФИО	Текстовое(50)	Единственное или основное написание Фамилии Имени Отчества репрессированного
3.	Suff	Суффикс	Текстовое(2)	Дополнение к ФИО
4.	KindN	Тип ФИО	Байт	**Р**усский, **Е**вропейский, **А**зиатский, **И**ной
5.	ABC	Алфавит	Байт	**Р**усский, **Л**атинский, **И**ной
6.	Sex	Пол	Текстовое(1)	М или Ж
7.	Birth-day	Дата рождения	Дата/время	1-е поле даты
8.	Year_of_birth	Год рождения	Целое	2-е поле даты
9.	Month_of_birth	Месяц рождения	Байт	3-е поле даты
10.	Day_of_birth	День рождения	Байт	4-е поле даты
11.	Year_of_birth1	Начало периода	Целое	5-е поле даты
12.	Year_of_birth2	Конец периода	Целое	6-е поле даты
13.	Comment_of_date	К дате	Мемо	7-е поле даты
14.	SDate	Источник даты	Байт	Локальный номер источника в анкете
15.	Birth-place	Место рождения	Длинное целое	Ссылка на справочник
16.	Comment	К биографии	Мемо	Примечание
17.	Family	Семья	Логическое	Данные на группу лиц
18.	Mark	Пометка	Логическое	Для работы с выборками анкет
19.	SourceM	Источник	Байт	Источник по умолчанию

Surname\ФИО2

В этой таблице находятся варианты фамилии, имени, отчества.

	Имя поля	Русское название	Тип поля	Комментарий
1.	Id	Номер записи	Счетчик	Ключ
2.	Rprid	Код репрессированного	Длинное целое	Для связи с Главной таблицей
3.	Source	Источник	Байт	Локальный номер источника в анкете
4.	Surname	ФИО	Текстовое(50)	Варианты Фамилии Имени Отчества
5.	Suff	Суффикс	Текстовое(2)	Дополнение к ФИО
6.	KindN	Тип ФИО	Байт	**Р**усский, **Е**вропейский, **А**зиатский, **И**ной
7.	TypeN	Тип именования	Байт	Другая фамилия, вариант написания, псевдоним, кличка, церковное имя
8.	ABC	Алфавит	Байт	**Р**усский, **Л**атинский, **И**ной
9.	Comment	К ФИО	Мемо	Примечание

DOB2\Дата рождения2

В этой таблице находятся варианты даты рождения.

	Имя поля	Русское название	Тип поля	Комментарий
10.	Id	Номер записи	Счетчик	Дубликат даты рождения
1.	Rpr_id	Код репрессированного	Длинное целое	Для связи с Главной таблицей
2.	Birth-day	Дата рождения	Дата/время	1-е поле даты
3.	Year_of_birth	Год рождения	Целое	2-е поле даты
4.	Month_of_birth	Месяц рождения	Байт	3-е поле даты
5.	Day_of_birth	День рождения	Байт	4-е поле даты
6.	Year_of_birth1	Начало периода	Целое	5-е поле даты
7.	Year_of_birth2	Конец периода	Целое	6-е поле даты
8.	Comment_of_date	К дате	Мемо	7-е поле даты
9.	SDate	Источник	Байт	Локальный номер источника в анкете

Death\Смерть

Эта таблица хранит сведения об обстоятельствах смерти репрессированного.

	Имя поля	Русское название	Тип поля	Комментарий
1.	Rpr_id	Код репрессированного	Длинное целое	Для связи с Главной таблицей
2.	Death-day	Дата смерти	Дата/время	1-е поле даты
3.	Year_of_death	Год смерти	Целое	2-е поле даты
4.	Month_of_death	Месяц смерти	Байт	3-е поле даты
5.	Day_of_death	День смерти	Байт	4-е поле даты
6.	Year_of_death1	Начало периода	Целое	5-е поле даты
7.	Year_of_death2	Конец периода	Целое	6-е поле даты
8.	Comment_of_date	Примечание к дате	MEMO	7-е поле даты
9.	SDate	Источник	Байт	Локальный номер источника в анкете
10.	Death-place	Место смерти	Длинное целое	Ссылка на справочник
11.	Burial place	Место захоронения	Целое	Ссылка на справочник
12.	Cause_of_death	Причина смерти	Байт	Ссылка на справочник
13.	Shooting	Расстрел	Логическое	Был ли расстрел
14.	Comment	К смерти	MEMO	Примечание

Source\Источники

Эта таблица хранит глобальный перечень использованных источников.

	Имя поля	Русское название	Тип поля	Комментарий
1.	SourceId	Код источника	Длинное целое	Уникальный код источника
2.	TypeS	Тип источника	Байт	Ссылка на справочник
3.	LangS	Язык источника	Байт	Ссылка на справочник

R_S\Репрессированный_Источник

Эта таблица связывает источники с анкетами.

	Имя поля	Русское название	Тип поля	Комментарий
1.	Number	Локальный источник	Байт	Локальный код источника
2.	Reprid	Код_репр	Длинное целое	Код анкеты
3.	Sourceid	Глобальный источник	Длинное целое	Глобальный код источника

Archinv\Архивно-следственные

Эта таблица хранит перечень использованных архивно-следственных дел.

	Имя поля	Русское название	Тип поля	Комментарий
1.	Id	Код источника	Длинное целое	Код источника в Source
2.	Arch	Архив	Целое	Ссылка на справочник архивов
3.	Year	Год	Целое	Год дела
4.	Fund	Фонд	Текстовое(8)	Номер фонда
5.	Inventory	Опись	Текстовое(8)	Номер описи
6.	Arch_num	Арх_ном	Текстовое(9)	Архивный номер дела / номер ед.хранения
7.	Vol	Том	Целое	Номер тома
8.	Page	Лист	Целое	Лист дела
9.	NInvest	След_ном	Текстовое(8)	Номер следственного дела
10.	Comment	Примечание к документу	MEMO	Примечание

Report\Сообщение (или Evidence\Свидетельство)

Эта таблица хранит перечень сообщений\свидетельств.

	Имя поля	Русское название	Тип поля	Комментарий
1.	Id	Код источника	Длинное целое	Код источника в Source
2.	Reprid	Код_репр	Длинное целое	Источник сообщения (репрессированный)
3.	Persid	Код_перс	Длинное целое	Источник сообщения (нерепрессированный)
4.	Relation	Отношение	Байт	Отношение к репрессированному
5.	Year	Год	Целое	Год сообщения
6.	Date	Дата	Дата\время	Дата сообщения
7.	Comment	Примечание к сообщению	MEMO	Примечание

БЕЗОПАСНОСТЬ СИСТЕМЫ

Необходим комплексный подход к проблеме безопасности. Сбои возможны в работе любой компьютерной системы. Однако, кроме сбоев программы или оборудования, может быть отключено электропитание, произойти пожар или другое непреодолимое бедствие. Не исключаются некорректные действия персонала, как непреднамеренные, так и преднамеренные (например, произведенные уволенным или недовольным сотрудником). Сама специфика проекта может спровоцировать политических противников и прочих недоброжелателей на деструктивные действия. Нельзя исключать возможности изменения законодательной базы, регламентирующей использование тех или иных информационных технологий. Наконец, сами сведения, составляющие тайну и хранимые в электронном виде, крайне трудно поддаются учету, весьма непросто обеспечить их конфиденциальность и целостность. Эти и многие другие факторы составляют угрозу безопасности.

Принято разделять эти угрозы на непреднамеренные и преднамеренные, рассматривая все их в тесной взаимосвязи друг с другом. Анализ архитектуры безопасности с применением различных моделей реализации угроз (анализа рисков, анализа сценариев, опросного анализа и пр.) позволяет достаточно точно и обоснованно определить приоритетные направления мероприятий по предотвращению угроз безопасности.

рис.5 Архитектура безопасности.

Вопросы обеспечения физической безопасности баз данных и их серверов решаются такими средствами: укрепленные помещения, охрана, видео наблюдение, надежное энергоснабжение, средства пожаротушения и пр.

Безопасность обслуживающего персонала обеспечивается соответствующим подбором, обучением, охраной труда и здоровья, мотивацией и психологическим сдерживанием, разграничением полномочий, проверками и пр.

Безопасность серверного оборудования обеспечивается выбором оборудования, его сертификацией и освидетельствованием на предмет закладок, размещением в защищенном помещении и экранированием, дублированием, резервным копированием, аппаратным управлением доступом и т.д.

Безопасность программного обеспечения достигается правильным выбором программных средств, верификацией, сертификацией, контролем целостности, антивирусной защитой и т.д.

Безопасность правового обеспечения достигается соответствующей законодательной базой и должностными инструкциями.

Более сложной проблемой является обеспечение безопасности баз данных в телекоммуникационной (сетевой) сфере. В данном проекте эта сфера образована телекоммуникационными сетями общего пользования (интернет). Стоимость несанкционированного доступа к транзакциям к базам данных в данной сфере невысока. Этот доступ можно легко реализовать при помощи специализированного программного и аппаратного обеспечения, а в ряде случаев стандартными средствами.

С точки зрения реализуемого проекта основными моментами обеспечения безопасности будут следующие:

- Обеспечение физической безопасности, целостности и сохранности данных ЕЭБД.
- Обеспечение безопасности ЕЭБД при взаимодействии с внешним миром (обеспечение аутентификации пользователей и обеспечение прав доступа, защита от несанкционированного доступа, защита от блокирования системы и т.п.).
- Обеспечение безопасности ЕЭБД на уровне поставляемых данных.

1. Физическая безопасность ЕЭБД

Физическая безопасность ЕЭБД будет обеспечиваться рядом технических и организационных мер. Для обеспечения сохранности данных предусматривается:

- Использование высококачественного оборудования и комплектующих ведущих производителей, имеющих сертификаты качества и соответствующего самым жестким требованиям.
- Использование кластерной архитектуры и возможностей работы ключевых программных продуктов в распределенной среде для снижения риска потери данных вследствие выхода из строя аппаратного обеспечения.
- создание резервных копий баз данных ЕЭБД на сменных носителях, во избежание потери данных вследствие отказа оборудования. Для этих целей в физическом дизайне системы предусмотрены аппаратные средства, позволяющие выполнять резервное копирование данных в соответствии с требованиями политики безопасности.
- создание резервных копий баз данных ЕЭБД в географически удаленных местах средствами репликации Microsoft SQL Server 2000, во избежание потери данных вследствие действия непреодолимых природных сил.

2. Безопасность ЕЭБД при взаимодействии с внешним миром.

Безопасность ЕЭБД при взаимодействии с внешним миром будет обеспечиваться:

- Использованием высококачественных и надежных аппаратных средств.
- Программными средствами, соответствующими требуемым классам надежности и степеням защиты.
- Организационными мерами, направленными на поддержание бесперебойного функционирования системы обеспечения безопасности.

Для обеспечения безопасности данных ЕЭБД от воздействий через интернет предлагается трехступенчатая система защиты, состоящая из аппаратной и 2-х программных частей. На аппаратном уровне функции защиты будет выполнять маршрутизатор, отделяющий ЕЭБД от внешнего мира, посредством контроля портов, используемых клиентами системы. Следующим этапом обеспечения безопасности будет фильтрация входящих/исходящих пакетов по критериям, определенным политикой безопасности, а также анализ активности и обнаружение внешних атак, реализуемые посредством Microsoft ISA Server. Второй программной ступенью защиты будут встроенные в серверную и клиентскую части средства шифрования/дешифрования передаваемых пакетов, а также средства контроля целостности. Аутентификация пользователей и предоставление прав доступа, базирующаяся на жесткой системной политике с четким разграничением и контролем прав выполняется средствами Microsoft Windows 2000 Server, Microsoft Internet Information Server и Microsoft SQL Server 2000. В качестве дополнительного способа обеспечения безопасности возможно использование защищенных сессий взаимодействия клиента и ЕЭБД, реализуемое посредством создания VPN-туннелей и SSL-соединений (см. рис.6).

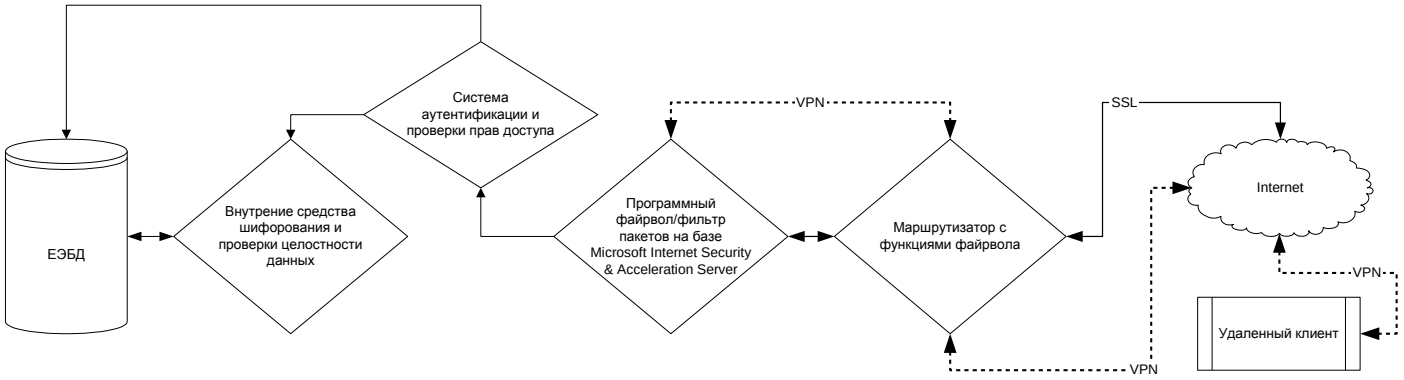


рис.6 Принципиальная схема обеспечения безопасности ЕЭБД

Для организации доступа к закрытым частям сайта наиболее приемлемым будет использование протокола SSL (см. приложение).

3. Обеспечение безопасности ЕЭБД на уровне поставляемых данных.

С нашей точки зрения, одними из наиболее эффективных средств обеспечения безопасности на уровне поставляемых данных являются криптографические средства, применяемые совместно с защищенными коммуникационными туннелями, программной и аппаратной защитой коммуникационных портов от несанкционированного использования или воздействия, что позволяет в большинстве случаев достичь нужного уровня безопасности.

Криптографические средства на основе шифрования с открытым ключом будут использоваться для обеспечения безопасности передачи пакетов с данными в ЕЭБД и исключения возможности подмены пакетов, с целью внесения некорректных данных в ЕЭБД. Схематическое описание использования криптографических средств приведено на рис. 7.

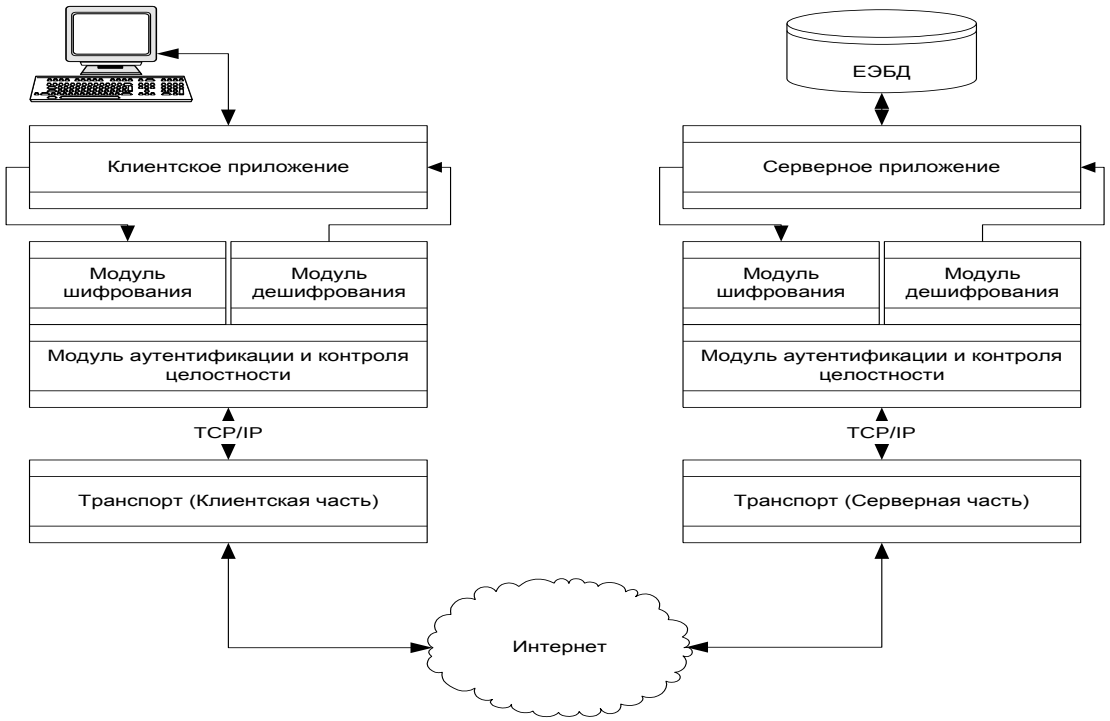


рис. 7 Принципиальная схема криптографического обеспечения безопасности ЕЭБД

Аппаратное обеспечение

На аппаратном уровне предлагается реализовать систему в кластерной архитектуре. Данная архитектура обеспечивает повышенную отказоустойчивость всего узла в целом, а также рассчитана на более высокую нагрузку, по сравнению с классической (не-кластерной) архитектурой. Более подробно с принципами работы и устройством кластерной архитектуры можно ознакомиться в приложении.

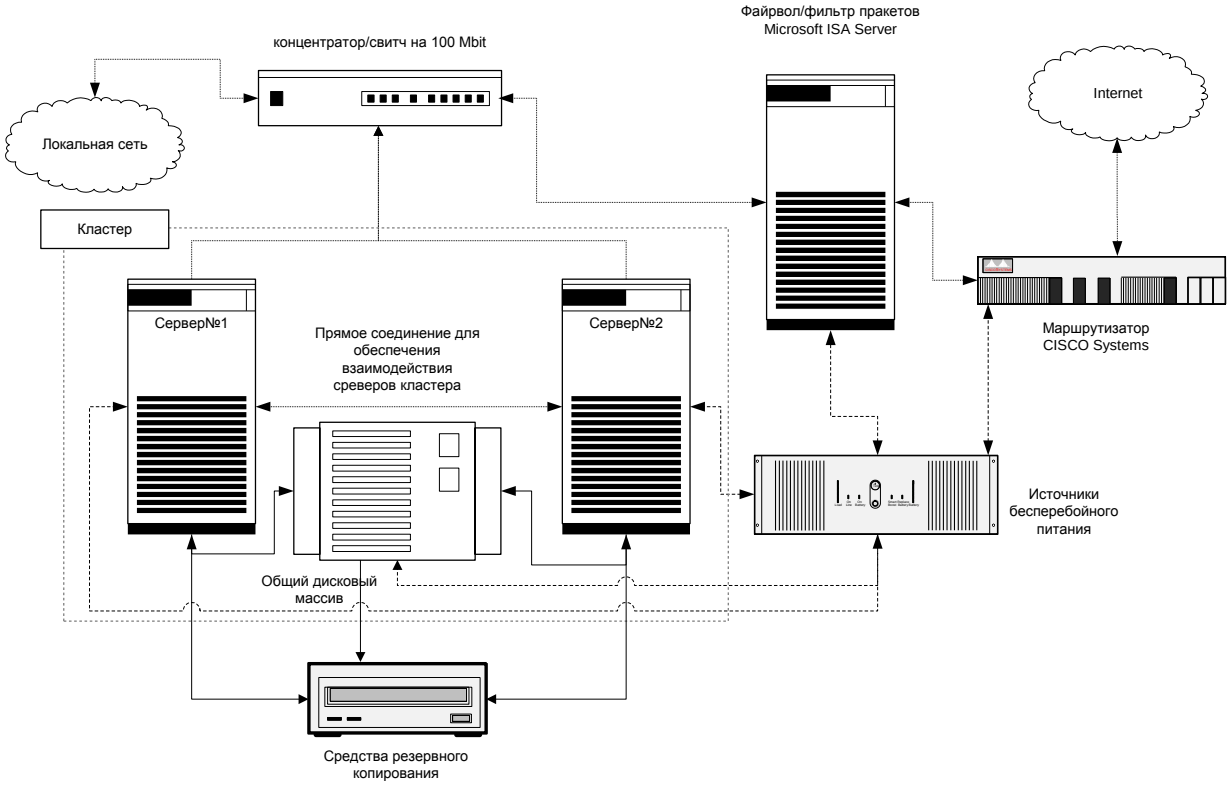


рис. 8 Схема аппаратного обеспечения центрального узла.

Пояснение к схеме на рис.8.

Обозначение на схеме	Описание
Сервер №1, №2	Специализированные сервера, работающие в составе кластера
ISA Сервер	Специализированный сервер, выполняющий функции защиты центрального узла.
Свитч/Концентратор	Концентратор, обеспечивающий взаимодействие кластера, серверов и компьютеров в локальной сети центрального узла.
Источники бесперебойного питания	Источники бесперебойного питания, обеспечивающие защиту компонентов узла и их работу в случае выхода из строя основной электросети
Маршрутизатор	Аппаратно-программный комплекс для организации сетевой защиты
Общий дисковый массив	Аппаратный комплекс повышенной отказоустойчивости, используемый кластером для хранения данных

DVD-RAM	Устройство для резервного копирования

Список оборудования необходимого для организации работы узла и его ориентировочная стоимость

(цены по данным системы www.price.ru на 05.2001)

Наименование	**Наименование оборудования**	**Цена $**	**Кол-во**	**Сумма $**
Сервер №1, №2	Dell Power Edge 4400 (x2) или Compaq ProLiant CL380	15000	1	15000
Общий дисковый массив	Power Edge Scalable Disk System (PSDS) Или Compaq Shared Storage RAID CR3500 Controller+Disks	10000	1	10000
Rack	Шкаф напольный 42U, 2033x800x600 мм	2000	1	2000
Switch HUB	CNET Fast Ethernet Switch 24x10/100Base-TX или 3Com SuperStack III Switch 3300 24x10/100Base-TX	1100	1	1100
ИБП	APC Smart-UPS 1400 XL Rack Mount w/PowerChute+	1200	2	2400
Файрвол/фильтр пакетов MS ISA Server	Dell PowerEdge 1400 или COMPAQ Proliant DL360R01	3500	1	3500
Расходные материалы и комплектующие	Мониторы, клавиатуры, картриджи DLT и другое…	1000	1	1000
DVD-RAM	Устройство для резервного копирования	1500	1	1500
Маршрутизатор	Cisco 2620 10/100 Ethernet Router with IOS Firewall Feature Set	3800	1	3800
Итого:				**40300**

При использовании оборудования других производителей или моделей сумма затрат может измениться в ту или другую сторону.

Маршрутизатор

Серия Cisco 2600 представляет собой новую надежную серию модульных маршрутизаторов, сочетающих в себе возможности серверов доступа и межсетевых экранов.

Основные возможности:

- Модульная архитектура
- Встроенные порты ЛВС
- Маршрутизация
- Межсетевой экран
- Полный набор сетевых протоколов
- Функции трансляции адресов (NAT), удаленного мониторинга (RMON), протокола резервирования ресурсов (RSVP)
- Шифрование на сетевом уровне с использованием стандартной технологии IPSec

Источники бесперебойного питания.

Серия Smart-UPS RM XL идеально подходит для приложений, где необходимо длительное время работы от батарей при отключении электричества. Это, прежде всего, сервера баз данных, обслуживающие крупные объемы данных, веб-сервера, требующие постоянной доступности для посетителей, телекоммуникационные системы.

Система резервного копирования

Для резервного копирования данных предлагается использовать DVD-RAM устройства с дисками емкостью 4,7 Гигабайта. Стоимость одного DVD-RAM диска около 50 $USA. Это, на наш взгляд, самый оптимальный вариант по организации резервного копирования, как по стоимости, так и по быстродействию, надежности и емкости носителей.

Преимущества кластерного варианта

Сегодня эффективность существования и реализации любого проекта напрямую зависит от работоспособности его информационной системы, и это диктует необходимость создания технологий, обеспечивающих безотказное функционирование вычислительных средств. Многие компании, которые в настоящее время применяют высокопроизводительные и относительно дешевые Intel-серверы с операционной системой Windows NT/2000, заинтересованы во внедрении кластерных решений, как для повышения надежности приложений, так и для повышения их масштабируемости.

Основным подходом к построению отказоустойчивых должен быть подход, предполагающий, что решение должно быть ниже стоимости устранения последствий отказов. Один из основных показателей надежности вычислительной системы - время ее безотказного функционирования в течение года.

Причины выхода из строя системы:

- Сбои программного обеспечения;
- Ошибки пользователей;
- Внешние факторы (пожары, землетрясения и т.д.);
- Аппаратные сбои;

Влияние окружающей среды можно минимизировать, разместив серверы, решающие общую задачу в рамках компьютерного кластера, на достаточном удалении друг от друга. Последствия аппаратных сбоев устраняются с помощью резервирования компонентов, которое осуществляется как на уровне вычислительных систем, так и их отдельных устройств. Принцип здесь такой: когда один из компонентов выходит из строя, вместо него включается резервный. Проблемы, связанные с программным обеспечением, решаются посредством "перепоручения" исполнения задачи другой машине. Что же касается ошибок пользователей, то их вероятность снижается при высоком уровне подготовки персонала и организации поддержки со стороны компании-производителя или поставщика вычислительных средств.

Для построения надежной компьютерной системы требуется комплексный подход, который подразумевает не только технологические инновации на программном и аппаратном уровнях, но и осуществление организационно-технических мероприятий, которые гарантируют эффективное использование этих инноваций клиентом.

Основные составляющие системы:

- Microsoft Cluster Server - кластерная технология для Intel-систем компании Microsoft для WindowsNT/2000;
- Сервера Dell PowerEdge, Compaq Proliant, Hewlett Packard (начиная от L-серии);
- Дополнительные сетевые адаптеры для создания межузловой (heartbeat) связи;
- Общее дисковое пространство серверов реализованное на базе технологии SCSI или Fibre Channel. (Диски распределяются между двумя серверами, на каждом из которых решается своя собственная задача);

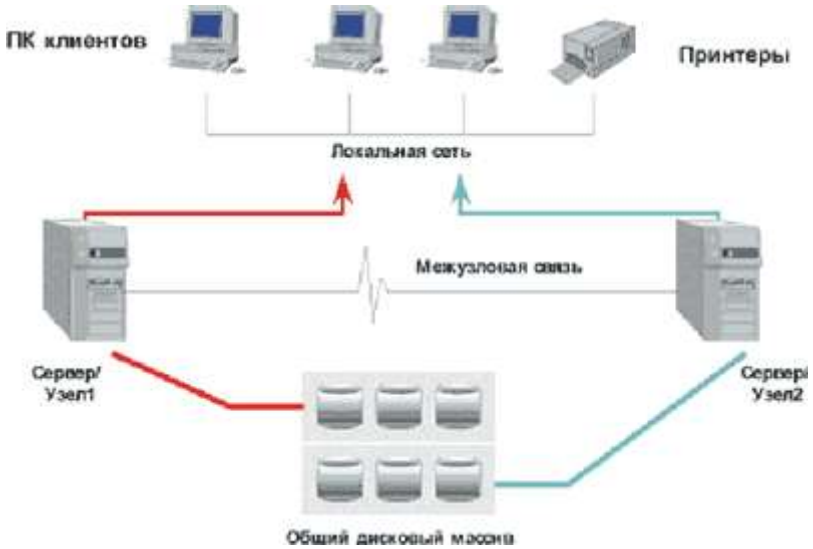


Рис 9. Структура кластера "Microsoft Cluster Server"

Принцип работы кластера:

Если один из серверов вследствие какого-то сбоя перестает отвечать на посылаемые ему запросы, ПО Microsoft Cluster Server организует исполнение его задачи на другой машине. В этом случае диски отказавшего сервера переходят в ведение работающего. Когда две задачи приходятся на один сервер, суммарная производительность вычислительной системы несколько снижается. Однако обе задачи продолжают выполняться, и есть возможность параллельно заниматься ремонтом вышедшего из строя компьютера. Период, в течение которого пользователь не имеет доступа к приложениям (так называемое "мертвое время"), незначителен - он длится, пока задача перемещается с одного сервера на другой.

Служба кластеров дает возможность соединения нескольких серверов в кластер, что обеспечивает высокую степень доступности и простоту управления данными и программами, работающими в пределах кластера. Служба кластеров обеспечивает в технологии кластеризации три принципиальных преимущества:

- **Улучшенная доступность**– благодаря тому, что в кластере серверов службы и приложения могут работать во время отказа аппаратного или программного компонента либо в процессе планового обслуживания.
- **Улучшенная масштабируемость**– благодаря поддержке серверов, в которые можно добавить несколько процессоров (до восьми процессоров в системе Windows 2000 Advanced Server) и дополнительную память (до 8 ГБ ОЗУ в системе Advanced Server).
- **Улучшенная управляемость**– благодаря предоставленной администраторам возможности управлять устройствами и ресурсами в пределах целого кластера как ресурсами одного компьютера.

Служба кластеров является одной из двух дополнительных технологий кластеров Windows, предлагаемых в качестве расширения базовых операционных систем Windows 2000 и Windows NT. Другая технология кластеров – балансировка сетевой нагрузки – дополняет службу кластеров путем поддержки высокодоступных и масштабируемых кластеров интерфейсных приложений и служб, таких, как узлы интернета или интрасети, веб-приложения, потоки мультимедиа.

Более подробно данный вопрос можно изучить на сайте Microsoft

Secure Sockets Layer (SSL) Protocol

Secure Sockets Layer (SSL) Protocol - промышленный протокол, использующий криптографию для обеспечения безопасности при передаче сообщений. Он используется в коммерческих клиентских и серверных приложениях ведущих мировых производителей для обеспечения безопасности сообщений. Стандарт SSL был разработан фирмой Netscape Communications (http://home.netscape.com/info/security-doc.html)

Три основные функции безопасности, гарантированные в SSL, основаны на криптографии с открытым ключом:

Конфиденциальность сообщений обеспечивается применением комбинированной схемы с использованием криптографии с открытыми и симметричными ключами. Весь поток сообщений между клиентом и сервером шифруются при помощи сессионного ключа, который был выработан на начальной стадии протокола SSL, называемой "handshake". Шифрование потока данных позволяет скрыть содержание сообщений даже при перехвате.

Достоверность и целостность сообщений обеспечивается электронной подписью. Электронная подпись—результат шифрования секретным ключом отправителя краткого содержания сообщения, вычисленного с помощью специальных математических функций. Расшифровать подпись может любой, знающий открытый ключ отправителя (он не является секретом), но, если даже злоумышленник и внесет изменения в текст, он не сможет изменить и вновь зашифровать электронную подпись, т.к. секретный ключ известен лишь отправителю.

Взаимная аутентификация позволяет клиенту убедиться в подлинности соединения с требуемым сервером, а серверу, при необходимости, убедиться в достоверности клиента. Это достигается путем взаимообмена сертификатами. Получив сертификат клиента, сервер заставляет его зашифровать своим секретным ключом случайное число, а затем расшифровывает сообщение клиента открытым ключом, указанным в сертификате. Эта процедура необходима, т.к. сам по себе сертификат не аутентифицирует клиента, он не секретный и передается по сети в открытом виде. Идентифицировать клиента можно только с помощью схемы, использующей сертификат и соответствующий секретный ключ клиента. Тот, кто обладает секретным ключом, и является действительным владельцем сертификата. По этой же схеме клиент может провести аутентификацию сервера.

Протокол шифрования SSL работает совместно с протоколом HTTP и не требует от пользователя каких-либо действий. При входе в шифрованные зоны вебсайтов, браузер автоматически устанавливает секретное соединение с веб-сервером и далее передача данных ведется с шифрованием всей информации.

Механизм работы протокола SSL. В течение "handshake" происходит следующее:

1. Клиент и сервер обмениваются своими сертификатами. Сначала сервер передает клиенту свой сертификат, если клиент отвечает, что гарант сертификата ему неизвестен, сервер передает сертификат гаранта либо свой сертификат от другого гаранта. Так продолжается до некоторого корневого сертификата, который должен поддерживаться и клиентом и сервером, в противном случае соединение разорвется.

2. Клиент вырабатывает сессионные ключи, которые будут использоваться для шифрования сообщений, и подписывает их. Ключи шифруются открытым ключом сервера, полученным из его сертификата, и передаются ему. Используются четыре ключа для одной SSL сессии. Клиент шифрует и расшифровывает посылаемые и получаемые сообщения разными ключами. Так же поступает и сервер.

3. Выбирается алгоритм шифрования сообщений и вырабатывания электронной подписи. Клиент предоставляет список алгоритмов, которые он понимает, а сервер из предоставленных алгоритмов выбирает наиболее строгий.

Конфиденциальность сообщений обеспечивается применением комбинированной схемы с использованием криптографии с открытыми и симметричными ключами. Достоверность и целостность сообщений обеспечивается электронной подписью. Взаимная аутентификация позволяет клиенту убедиться в подлинности соединения с требуемым сервером, а серверу, при необходимости, убедиться в достоверности клиента. Это достигается путем взаимообмена сертификатами.