УТВЕРЖДЕНО
Старший вице-президент – директор по проектированию ОАО «НИАЭП»

_____ Ю.А. Иванов
« ___ » _____ 2013 г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ
по теме:
«Разработка и внедрение подсистемы обеспечения информационной безопасности ЕОНКОМ»

СОГЛАСОВАНО:
Начальник Отдела информационных технологий

_____ Е.Ф. Пашенцева
(подпись, дата)

Заместитель директора московского филиала
_____ В.В. Аленьков
(подпись, дата)

РАЗРАБОТАНО:
Начальник Управления информационных проектов развития

_____ И.Д. Уваров
(подпись, дата)

Начальник Отдела разработки структур каталогов
_____ М.Ю. Корытов
(подпись, дата)

Инженер 3к. Отдела разработки структур каталогов

_____ А.В. Сидоров
(подпись, дата)

Нижний Новгород,
2013г.

Оглавление

1. Термины и сокращения

-

Автоматизированная система (Система) – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Информационная безопасность – обеспечение конфиденциальности, целостности и доступности информации; также могут подразумеваться другие свойства, такие как аутентичность, подотчетность, неотказуемость и надежность.

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

Корпоративная сеть передачи данных – технологическая система, предназначенная для передачи по линии связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Подсистема обеспечения информационной безопасности ЕОНКОМ (Подсистема) – комплекс организационных мер и программно-технических (в том числе криптографических) средств обеспечения безопасности информации в автоматизированных системах.

2. Общие сведения

2.1. Наименование работ по проекту

Разработка и внедрение подсистемы обеспечения информационной безопасности ЕОНКОМ.

2.2. Номер проекта

2.3. Наименование Заказчика и Исполнителя работ по проекту

Заказчик – Открытое акционерное общество «Нижегородская инжиниринговая компания «Атомэнергопроект».

Исполнитель – определяется по результатам конкурентной процедуры закупки в соответствии с Единым отраслевым стандартом закупок (положением о закупке) Государственной корпорации по атомной энергии «Росатом».

2.4. Перечень документов, на основании которых создается Подсистема

Отраслевой стандарт обеспечения информационной безопасности Госкорпорации «Росатом».

2.5. Сроки выполнения работ:

Работы должны быть выполнены в течение 4-х месяцев с момента заключения Договора.

2.6. Сведения о порядке финансирования работ

Финансирование выполненных Исполнителем работ осуществляется в соответствии с договором между Исполнителем и Заказчиком.

2.7. Порядок оформления и предъявления Заказчику результатов работ

Порядок оформления и предъявления Заказчику результатов работ по созданию Системы определяется договором между Исполнителем и Заказчиком и его приложением - Календарным планом.

3. Назначение и цели создания (развития) Системы

3.1. Назначение Подсистемы обеспечения информационной безопасности

Назначением выполнения работ по проекту «Разработка и внедрение подсистемы обеспечения информационной безопасности ЕОНКОМ» является обеспечение информационной безопасности ЕОНКОМ от внутренних или внешних угроз.

3.2. Цели создания Подсистемы обеспечения информационной безопасности

Обеспечение:

- конфиденциальности информации Системы ЕОНКОМ (защита от утечки, разглашения информации ограниченного доступа);
- целостности информации Системы ЕОНКОМ (защита информации от искажения и уничтожения);
- доступности информации Системы ЕОНКОМ (защита от блокировки доступа к информации пользователями).

Защита информации Системы ЕОНКОМ обеспечивается реализацией комплекса организационных и технических мер и внедрением программно-аппаратных средств защиты информации, устраняющих или значительно снижающих угрозы для Системы ЕОНКОМ.

4. Характеристики объекта автоматизации

4.1.Краткие сведения об объекте автоматизации

4.1.1. Рабочая среда Системы ЕОНКОМ

Рабочей средой Системы является Enovia V6 - гибкая PLM-система компании Dassault Systems (Франция). Enovia V6 позволяет производить ее настройку под решаемый спектр задач и обеспечивает работу с большими объемами информации, что очень актуально с учетом большого оборудования и материалов, поставляемых на АЭС. При этом Enovia V6 дает возможность одновременной работы большого количества пользователей в Каталоге, при наличии доступа в Интернет и установленного web-браузера.

4.1.2. Основные участники процесса информационного обмена в Системе ЕОНКОМ

– Заказчик - компания, разместившая заказы на строительство АЭС, управляющая сроками и стоимостью строительства, а так же проводящая оценку качества используемого оборудования и материалов в процессе эксплуатации объектов;

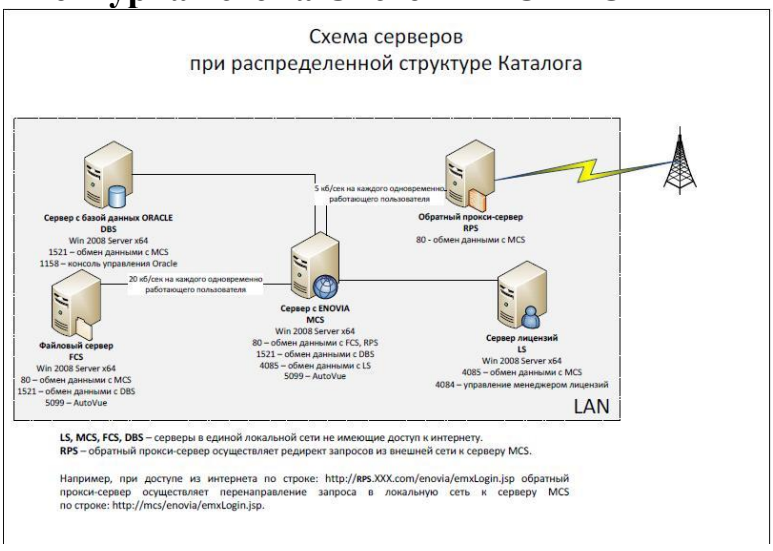
– Поставщики оборудования и материалов – компании, поставляющие свою продукцию для атомной отрасли и размещающие информацию о ней в Системе;

– Проектные и конструкторские компании – компании, осуществляющие проектирование и строительство новых объектов АЭС и получающие из Системы информацию о технических параметрах оборудования, и о возможных поставщиках;

– Оператор АЭС - компания, осуществляющая эксплуатацию АЭС и получающая из Системы информацию об эксплуатационных характеристиках установленного оборудования;

– Верификатор (ОАО «НИАЭП») - компания, являющаяся центром верификации данных и осуществляющая техническую поддержку Системы.

4.1.3. Архитектурная схема Системы ЕОНКОМ



4.2.Сведения об условиях эксплуатации Системы

В ходе эксплуатации Система должна быть способна к интеграции в свою среду новых подсистем, расширения функций уже имеющихся, а так же допускающая свою интеграцию в состав более крупных «охватывающих» информационных комплексов. Данный принцип требует соблюдения принятых к реализации стандартов и мер обеспечения информационной безопасности.

Система должна обеспечивать на каждом уровне санкционированный доступ к информации в соответствии с матрицей доступа. Это означает, что ту или иную информацию пользователь может получить от системы только в соответствии с установленными для него правами (на создание, на чтение, на модификацию, на уничтожение данных и т.п.). Эти права устанавливаются администратором системы на основе документов, регламентирующих правила пользования информацией, циркулирующей в системе. Данный принцип предъявляет определенные требования к степени защиты информации в каналах связи, локальных вычислительных сетях, на отдельных ПВЭМ, входящих в состав программно-технического обеспечения системы.

5. Требования к Подсистеме информационной безопасности

5.1. Требования к Подсистеме в целом

5.1.1. Требования к структуре и функционированию подсистемы

5.1.1.1. Перечень подсистем, их назначение и основные характеристики

Подсистема обеспечения информационной безопасности ЕОНКОМ.

5.1.1.2. Требования к способам и средствам связи для информационного обмена между компонентами системы:

Состав данных для информационного взаимодействия и способы реализации интерфейсов взаимодействия между системами должны отвечать разрабатываемым стандартам и мерам информационной безопасности.

5.1.1.3. Требования к характеристикам взаимосвязей создаваемой системы со смежными системами, требования к ее совместимости, в том числе указания о способах обмена информацией (автоматически, пересылкой документов, по телефону и т. п.)

Должна быть встроена в Систему обеспечения информационной безопасности корпоративной информационной сети ОАО «НИАЭП» и совместима с подсистемами ИБ, которые действуют в корпоративной информационной сети ОАО «НИАЭП»:

- Подсистема криптографической защиты сетевого трафика (ПАК CSP VPN Gate);
- Подсистема антивирусной защиты (на базе сертифицированного программного обеспечения, входящего в комплект Kaspersky Business Space Security);
- Подсистема анализа защищенности (на базе программного обеспечения MaxPatrol);
- Подсистема защиты рабочих станций и серверов от НСД (на базе программного обеспечения Secret Net 6).
- Подсистема защищенного доступа к ресурсам сети Интернет (Websense Data Security).

5.1.1.4. Требования к режимам функционирования системы

Система должна функционировать непрерывно круглосуточно. Под непрерывным режимом работы Системы понимается режим работы, при котором Система постоянно находится во включенном состоянии за исключением времени, необходимого для ее планового и внепланового технического обслуживания.

Подсистема обеспечения информационной безопасности должна функционировать в комплексе Системы и отвечать режиму работы Системы.

Система должна поддерживать многопользовательский режим работы.

5.1.1.5. Требования по диагностированию системы

Требования не предъявляются.

5.1.1.6. Перспективы развития, модернизации подсистемы

Принцип построения Подсистемы должен предусматривать возможности для развития и модернизации Подсистемы.

Развитие и совершенствование Подсистемы является необходимым условием ее существования, т.к. постоянно совершенствуются, изменяются и развиваются бизнес-процессы организации и ее подразделений, вовлеченных в процессы капитального строительства.

5.1.2. Требования к численности и квалификации персонала системы и режиму его работы:

5.1.2.1. Требования к численности персонала (пользователей) Системы:

Численность персонала Подсистемы должны определяться с учетом следующих требований:

- быть достаточной для реализации автоматизированных функций Подсистемы во всех режимах ее работы;
- быть достаточной для обеспечения бесперебойного функционирования Подсистемы.
- структура и конфигурация Подсистемы должны быть спроектированы и реализованы с целью минимизации количественного состава обслуживающего персонала;
- структура Подсистемы должна предоставлять возможность управления всем доступным функционалом Системы как одному администратору, так и предоставлять возможность разделения ответственности по администрированию между несколькими администраторами;

Количество и состав пользователей Системы определяется на этапе подготовки персонала объектов автоматизации и фиксируется в списке пользователей Системы и матрице доступа.

5.1.2.2. Требования к квалификации персонала, порядку его подготовки и контроля знаний и навыков:

Квалификация персонала должна обеспечивать качественное и эффективное функционирование программных средств Подсистемы во всех режимах работы.

Для администрирования Подсистемы к администратору не должны предъявляться требования по знанию всех особенностей функционирования элементов, входящих в состав администрируемых компонентов Подсистемы.

5.1.2.3. Требуемый режим работы персонала АС:

Аппаратно-программный комплекс Подсистемы не должен требовать круглосуточного обслуживания и присутствия администраторов у консоли управления.

Режим работы персонала Подсистемы должен обеспечивать своевременное выполнение всех операций в Подсистеме согласно регламентам выполнения операций в Подсистеме.

5.1.3. Показатели назначения

5.1.3.1. Степень приспособляемости Системы к изменению процессов и методов управления, к отклонениям параметров объекта управления:

Подсистема должна предусматривать возможность масштабирования по производительности и объему обрабатываемой информации без модификации ее программного обеспечения путем модернизации используемого комплекса технических средств. Возможности масштабирования должны обеспечиваться средствами используемого базового программного обеспечения.

5.1.3.2. Допустимые пределы модернизации и развития системы:

Без ограничений.

5.1.3.3. Вероятностно-временные характеристики, при которых сохраняется целевое назначение системы:

Аппаратно-программный комплекс Подсистемы должна обеспечивать:

- полноту покрытия функциональных требований к Подсистеме;
- отсутствие повторного ввода информации, если это не противоречит требованиям проверки достоверности информации;
- одновременную работу всех подключенных к Системе пользователей (многопользовательский режим работы), в т.ч. территориально удаленных друг от друга;
- продуктивное использование Системы не менее трех лет с момента ввода в эксплуатацию без необходимости перехода на новую версию.

5.1.4. Требования к надежности

5.1.4.1. Состав и количественные значения показателей надежности для системы в целом или ее подсистем:

Система должна сохранять работоспособность и обеспечивать восстановление своих функций при возникновении следующих внештатных ситуаций:

- при сбоях в системе электроснабжения аппаратной части, приводящих к перезагрузке ОС, восстановление программы должно происходить после перезапуска ОС и запуска исполняемого файла Системы;
- при ошибках в работе аппаратных средств (кроме носителей данных и программ) восстановление функции системы возлагается на ОС;
- при ошибках, связанных с программным обеспечением (ОС и драйверы устройств), восстановление работоспособности возлагается на ОС.

5.1.4.2. Перечень аварийных ситуаций, по которым должны быть регламентированы требования к надежности, и значения соответствующих показателей:

Без ограничений.

5.1.4.3. Требования к надежности технических средств и программного

обеспечения:

Требования не предъявляются.

5.1.4.4. Требования к методам оценки и контроля показателей надежности на разных стадиях создания системы в соответствии с действующими нормативно-техническими документами:

Требования не предъявляются.

5.1.5. Требования безопасности

Требования не предъявляются.

5.1.6. Требования к эргономике и технической эстетике

Подсистема должна обеспечивать эффективную и производительную работу.

Подсистема должна обладать логичной для пользователя навигацией, четкими для понимания текстами и значениями пользовательского интерфейса. Работа пользователя должна поддерживаться наличием вспомогательных средств (поисковых, справочных, нормативных, значений по умолчанию и пр.)

Для быстрого обучения пользователей работе с Подсистема необходимо использовать преимущественно стандартные элементы взаимодействия и их традиционное или общепринятое расположение.

К разрабатываемому интерфейсу пользователя предъявляются следующие требования:

- минимальный отклик системы;
- оптимизация интерфейса системы с точки зрения максимальной скорости работы с системой;
- унификация расположения управляющих элементов;
- подтверждения исполнения критических действий в системе.

5.1.7. Требования к транспортабельности для подвижных АС

Для работы с ЕОНКОМ запрещается использовать отчуждаемые накопители и носители информации.

5.1.8. Требования к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов системы

Система должна быть рассчитана на эксплуатацию в составе программно–технического комплекса Заказчика и учитывать разделение ИТ инфраструктуры Заказчика на внутреннюю и внешнюю. Техническая и физическая защита аппаратных компонентов системы, носителей данных, бесперебойное энергоснабжение, резервирование ресурсов, текущее обслуживание реализуется техническими и организационными средствами, предусмотренными в ИТ инфраструктуре Заказчика.

Обслуживающий персонал Подсистемы должен обеспечивать поддержание технических и программных средств Подсистемы в работоспособном состоянии во всех режимах функционирования, а также выполнять периодическое обслуживание и ремонтные работы.

Задачи, выполняемые обслуживающим персоналом:

- администрирование аппаратно-программного комплекса

Подсистемы и прикладных программных средств;

- обслуживание технических средств;
- обеспечение резервного копирования данных и восстановление данных в случае сбоев;
- централизованная поддержка пользователей Подсистемы.

Численность персонала должна быть достаточной для реализации задач по обслуживанию Подсистемы.

Количество и состав обслуживающего персонала Подсистемы определяется на этапе подготовки персонала объектов и фиксируется в Списке обслуживающего персонала Подсистемы.

5.1.9. Требования к защите информации от несанкционированного доступа:

В Системе должна быть обеспечена защита информации (хранимой, отображаемой, передаваемой) от всех следующих видов угроз:

- нарушение конфиденциальности;
- нарушение целостности;
- нарушение доступности.

Система должна обеспечивать информационную безопасность как от непреднамеренных или случайных действий, так и от преднамеренных угроз – несанкционированное получение информации и несанкционированная манипуляция данными, ресурсами и самой Системой.

Информационная безопасность должна строиться на основании применения:

- на автоматизированных рабочих местах и серверах, обеспечивающих функционирование Системы:
  - авторизацию пользователей путем идентификации и аутентификации по логину и паролю;
  - разграничение прав на основании ролей и полномочий в соответствии с матрицей доступа;
  - средств защиты от несанкционированного доступа;
  - средств антивирусной защиты;
  - средств резервного копирования и аварийного восстановления информации.
- для интерфейсов, обеспечивающих взаимодействие Системы с внешними Системами:
  - межсетевых экранов;
  - средств обнаружения вложений;
  - сертифицированных устройств криптографической защиты при передаче информации по сетям общего пользования типав Интернет.

В Системе должна быть предусмотрена регистрация действий пользователей и администраторов, контроль несанкционированного доступа и действий пользователей, администраторов и посторонних лиц, в т.ч. регистрация входа (выхода) в систему (из системы) либо регистрация загрузки и инициализации операционной системы и ее программного останова.

5.1.10. Требования по сохранности информации при авариях

Сохранность информации при авариях оборудования должна обеспечиваться за счет создания резервных копий хранилищ данных (семантических и пространственных), использования механизма транзакций.

Сохранность информации в Системе должна быть обеспечена за счет:

- хранения данных на отказоустойчивых RAID-массивах;
- использования механизмов транзакций;
- исключения несанкционированного доступа к данным;
- организации бесперебойного электропитания серверов;
- создания резервных копий хранилищ данных;
- восстановления данных из резервных копий в случаях сбоев.

Резервное копирование должно осуществляться средствами СУБД, под управлением которых размещаются хранилища данных подсистемы.

В комплект технической документации на программные компоненты подсистемы должны входить методики и регламенты резервного копирования данных, а также сведения о применимости механизмов транзакций (указанная информация может быть включена разделами в руководство администратора и/или другие документы).

Программное обеспечение Системы (включая разрабатываемую Подсистему информационной безопасности) должно восстанавливать свое функционирование при корректном перезапуске аппаратных средств.

5.1.11. Требования к защите от влияния внешних воздействий

Требования не предъявляются.

5.1.12. Требования к патентной чистоте

Требования к патентной чистоте исполнения настоящего Технического задания обеспечиваются в соответствии с договором между Исполнителем и Заказчиком.

5.1.13. Требования по стандартизации и унификации.

Требования по стандартизации и унификации программных средств Подсистемы должны быть обеспечены за счет применения унифицированных компонентов и средств из состава:

- операционных систем;
- систем управления базами данных;
- базового и прикладного программного обеспечения;
- стандартных графических интерфейсов разрабатываемых компонентов Подсистемы.;

Требования по стандартизации и унификации технических средств разрабатываемой Подсистемы должны быть обеспечены за счет использования серийно выпускаемых средств вычислительной техники и коммуникационного оборудования.

Проектирование, документирование и разработка Подсистемы должны производиться с соблюдением требований действующих государственных стандартов, в частности комплекса стандартов и руководящих документов на

автоматизированные системы управления, информационные технологии и процессы жизненного цикла систем: ГОСТ 31.201-89, ГОСТ 34.601-90, ГОСТ 34.602-89, ГОСТ 34.603-92, РД 50-34.698-90, ГОСТ Р ИСО/МЭК 15288-2005, ГОСТ Р ИСО/МЭК 12207-99, ГОСТ Р ИСО/МЭК 15910-2002, ГОСТ Р 51904-2002 и т.д.

5.1.14. Дополнительные требования.

Дополнительные требования не предъявляются.

5.2. Требования к функциям (задачам), выполняемым Подсистемой

5.2.1. Требования к функциональной архитектуре

Подсистема безопасности АС должна работать на уровне ядра АС таким образом, чтобы ни одно значимое действие в рамках системы – будь то действие пользователя или процесса – не происходило без участия подсистемы безопасности.

Схема безопасности, реализованная в Системе, должна быть отделена от средств безопасности самой операционной системы, на которой будет реализована АС, в том смысле, что сбой или уязвимость подсистемы безопасности операционной системы не должны влиять на работу подсистемы безопасности АС.

Механизмы безопасности подсистемы должны быть реализованы в форме широко известных в мире, опробованных и одобренных стандартов и протоколов.

Подсистема безопасности должна обеспечивать замкнутое сохранение данных, связанных с АС (собственно модулей системы, системных и прикладных данных) таким образом, чтобы:

- невозможно было получить логический доступ к указанным данным вне рамок работы приложения АС;
- любые перемещения данных из/в систему происходили под контролем подсистемы безопасности.

5.2.2. Требования к идентификации и аутентификации

Работа любого субъекта (пользователя или процесса) в АС должна быть идентифицирована Подсистемой информационной безопасности.

Основным средством аутентификации пользователей в АС должна быть схема «имя пользователя/пароль», при этом Система должна допускать возможность расширения процедур аутентификации на основе смарт-карты, touch memory. При этом должна присутствовать возможность дифференцированного считывания информации с токена – пароля или ПИН-кода при аутентификации, ключа при шифровании или электронно-цифровой подписи.

Парольная политика должна предусматривать возможность настройки по следующим параметрам:

- минимальная длина пароля;
- минимальный срок жизни пароля;

- максимальное количество ошибок при вводе пароля;
- поддержка истории паролей;
- определение примитивных и слабых паролей;
- требование ввода старого пароля при замене новым паролем;
- возможность изменить пароль пользователя, кроме него самого, должен иметь администратор безопасности, при этом он не должен иметь возможности получить информацию о старом, заменяемом пароле;
- при входе пользователя в систему должно присутствовать предупреждение о запрете использования чужих паролей и несанкционированного доступа;
- при входе пользователя в систему ему должна быть представлена информация о предыдущем успешном входе в систему (дата и время), а также количество ошибок при вводе пароля между двумя последними успешными входами в систему (если таковые были) с указанием даты и времени.

5.2.3. Требования к авторизации и доступу

Для определения единообразного уровня доступа субъектов к информационным объектам, являющимся первичной информационной единицей, система должна предусматривать возможность следующего распределения доступа:

- к группе или нескольким группам объектов;
- к объекту;
- к набору частей объекта.

Доступ к информационным объектам должен включать следующие виды ограничений:

- нет доступа к объекту;
- доступ (к объекту/части объекта) только на чтение;
- доступ (к объекту/части объекта) только на изменение - отдельно с чтением и без чтения;
- удаление информационного объекта (объекта Системы);
- добавление информационного объекта (объекта Системы);
- разрешение доступа на чтение;
- разрешение доступа на изменение;
- разрешение доступа на добавление;
- разрешение доступа на удаление.

Кроме доступа к конкретным информационным объектам, должно быть предусмотрено разделение доступа к функциям, выполняющим процессы над объектами. Отдельно должны быть выделены функции, выполняющие массовые изменения данных в информационных объектах.

Схема определения доступа должна предусматривать возможность группового или ролевого доступа, то есть создание абстрактного профиля прав пользователя. При включении нового пользователя в конкретную группу он

автоматически должен наследовать все права, присущие пользователям данной группы. При этом суммарные права пользователя должны проверяться на непротиворечивость, должен применяться принцип поглощения более широкими разрешительными правами более узких (суммирование прав). Также должна присутствовать возможность копирования (наследования) прав пользователя с возможностью последующей корректировки.

Для каждого информационного объекта должен существовать владелец объекта (с возможностью в дальнейшем заменить одного владельца на другого) с полными правами доступа. Система должна контролировать обязательное наличие хотя бы одного пользователя (владельца или администратора) для каждого информационного объекта.

Пользовательский интерфейс настройки прав доступа должен быть прост и интуитивно понятен.

5.2.4. Требования к конфиденциальности данных безопасности и прочих данных

Информация о критических атрибутах профиля пользователя (пароли) должна сохраняться в виде, исключающем возможность прямого доступа к ним пользователей, минуя средства системы, причем как для постоянной, так и для оперативной памяти. Это означает, что указанные данные при постоянном хранении должны быть защищены средствами криптографии с предоставлением доступа только либо самому пользователю, либо процессам подсистемы безопасности, либо администратору, уполномоченному подсистемой безопасности. При хранении данных в оперативной памяти должна исключаться возможность получения несанкционированного доступа к ним.

При этом пароли должны сохраняться в виде хеш-значений, а ключи – иметь возможность аварийного доверенного восстановления.

Система при передаче данных по каналам связи от места хранения до конечного пользователя в рамках локальной сети должна использовать только защищенное соединение, при этом защита должна быть осуществлена минимум на транспортном, предпочтительнее – на сетевом уровне.

5.2.5. Требования к целостности данных

АС должна поддерживать логическую целостность бизнес-данных, то есть изменения должны носить характер транзакционно-ориентированных, выполняющихся в целом от начала до конца либо, в случае сбоя, не выполняющихся совсем. При этом каждая транзакция должна проверяться на непротиворечивость в соответствии с настраиваемыми в АС правилами. Прохождение транзакции в АС должно быть разбито на этапы, сопровождаемые настраиваемым количеством подтверждений (ввод, авторизация и пр.)

Способы же авторизации транзакций должны настраиваться по выбору организации:

- несколько авторизаторов для одного пользователя;

- один авторизатор для группы пользователей;
- один авторизатор для данного типа операций.

Также должна присутствовать возможность включения/исключения полей записей транзакции в/из группы параметров для цифрового подписания.

Система должна иметь собственную встроенную или внешнюю подсистему проверки целостности файлов, модулей и системных данных самой АС на предмет их несанкционированной модификации.

Никакие системные или прикладные данные не должны удаляться в рамках АС без следов. Должна присутствовать настройка на запрет удаления отдельных категорий данных. Система также должна фиксировать информацию, необходимую для идентификации факта, объекта и субъекта процесса удаления. Система должна предусматривать возможность восстановления удаленных данных в течение определенного промежутка времени.

5.2.6. Требования к доступности данных

АС должна предусматривать возможность устойчивой работы при появлении сбоев (должна быт создана система из двух одинаковых комплектов серверов между которыми налажена репликация, при выходе из строя одного из комплектов в течении 5 минут должен быть осуществлен переход на резервный комплект серверов)

Процессы, требующие от системы монопольного использования ресурсов и препятствующие интерактивной работе пользователей, должны быть перенесены на время наименьшей активности (ночь) и в сумме занимать не более 10-15% суточного рабочего времени системы.

Система должна быть реализована в трехуровневой архитектуре клиент-сервер с тем, чтобы вывод из строя рабочего места пользователя или получение злоумышленником несанкционированного доступа к нему не сказывался на работе серверной части системы, а сбой сервера приложений не влиял на состояние данных системы.

Система должна обладать возможностью балансирования нагрузки между отдельными узлами, модулями и функциями, а также иметь подсистему предупреждения о работе в режиме, приближенном к максимальной загрузке.

АС должна иметь возможность резервного копирования и восстановления средствами самой системы. Резервное копирование должно осуществляться на различные носители по выбору организации, в том числе в дискретном (разорванном) виде, то есть общий объем резервной копии может быть распределен между двумя или более носителями меньшего объема.

Резервное копирование должно предусматривать как сохранение прикладных, так и системных данных, и осуществляться в режиме с криптографической защитой по заранее установленному графику от одного до нескольких раз в день либо вручную по команде оператора. При этом процедура не должна забирать ресурсы системы в монопольное использование.

В системе следует предусмотреть механизм облегченного восстановления потерянных в результате сбоя операционных данных со времени последнего

резервного копирования (время восстановления должно быть не более 30 минут).

5.2.7. Требования к удаленной работе

Система должна предусматривать возможность работы пользователей в удаленном режиме по выделенным, коммутируемым каналам либо средствами Интернета. Для этого она должна иметь либо собственную встроенную систему создания виртуальной частной сети, либо возможность тесной интеграции с межсетевым экраном.

В случае реализации защиты соединения на уровне выше сетевого система должна обладать защитой системы маршрутизации сетевых пакетов.

Системы настройки аутентификационных механизмов, авторизации, прав доступа и прочих элементов схемы безопасности должны четко различать варианты локальной и удаленной работы и, соответственно, иметь возможность применения различных правил в зависимости от режима доступа.

5.2.8. Требования к аудиту и мониторингу

Система аудита АС должна различать бизнес-значимые и системно-значимые события. Для бизнес-значимых событий должны фиксироваться параметры, которые не отражаются напрямую в прикладных данных системы, например такие, как время запуска процедуры массовой работы со счетами, имя пользователя и сетевой адрес его рабочей станции. Для системно-значимых событий должна происходить фиксация любых изменений, которые так или иначе могут отразиться на работе системы. Такой список должен включать следующие события (но не ограничиваться ими):

- добавление, удаление пользователя или изменение атрибутов пользователя;
- изменение настроек криптографической защиты данных;
- изменение настроек контроля целостности;
- изменение настроек удаленного доступа;
- изменение настроек резервного копирования;
- изменение настроек, влияющих на работоспособность и производительность системы;
- запуск, остановка процедур системного характера и обмен данными с процедурами системного характера;
- сообщения администратору, имеющие отношение к безопасности системы.

При этом информация, фиксируемая в регистрационных журналах, должна обеспечивать однозначную идентификацию субъекта, причины, времени, местоположения и результата произведенного действия.

Все бизнес-значимые действия пользователей в АС, как успешные, так и неудачные, начиная от попытки установления связи и до завершения сессии, должны быть зафиксированы. Журнал будет использован для исследования корректности работы АС, мониторинга действий пользователей, расследования

сложных или подозрительных событий и т. д.

Все события должны быть разбиты на типы и категории.

Каждый тип событий характеризуется уровнем доступа или тем, интересы каких пользователей могут затронуть события данного типа и для кого они будут доступны при просмотре журнала. Возможны следующие уровни:

- система в целом - уровень центрального администратора системы (доступны все события в системе);
- сотрудник - уровень сотрудника филиала (доступны только те события, которые относятся к нему или затрагивают его интересы);

Каждое событие должно обладать как минимум следующими реквизитами:

- автор (пользователь, который породил это событие);
- время (календарная дата и время, когда событие произошло);
- категория события;
- название события;
- объект события;
- описание события (конкретные подробности события и объекта);
- филиал организации, затронутый событием.

При работе с журналом событий должна быть обязательно предусмотрена возможность фильтрации событий, то есть возможность показывать не все события, соответствующие данному периоду, а только те, которые в настоящий момент нужны. Список параметров фильтрации должен включать все указанные выше реквизиты событий.

Регистрационные журналы системы должны обладать возможностью защиты от изменений со стороны любого субъекта, кроме процесса его формирования (доступ только на чтение уполномоченным администраторам). Доступ на чтение регистрационного журнала должен зависеть от установленного для данного администратора фильтра прав.

Регистрационный журнал должен обладать механизмами обеспечения его юридической доказательности (например, системная или административная цифровая подпись).

Аудит событий должен включать возможность формирования шаблонов событий, подозрительных на злоумышленные. При наступлении событий, соответствующих такому шаблону, система должна выдавать оповещение уполномоченному лицу.

Система должна предусматривать мониторинг и управление работой пользователей, включая следующие возможности:

- отображение текущих сессий пользователей в системе;
- отправка системного или административного сообщения пользователю или группе пользователей;
- автоматическое завершение сессии пользователя при достижении определенного времени бездействия в системе;

ручное принудительное завершение сессии пользователя (группы пользователей) администратором.

5.3. Требования к видам обеспечения

5.3.1. Требования к математическому обеспечению системы:

Математические методы и алгоритмы, используемые для шифрования/дешифрования данных, а также программное обеспечение, реализующее их, должны быть сертифицированы уполномоченными организациями для использования.

5.3.2. Требования к информационному обеспечению системы:

5.3.2.1. Состав, структура и способы организации данных в Подсистеме

Состав, структура и способы организации данных в Подсистеме должны быть определены на этапе технического проектирования.

Средства СУБД, а также средства используемых операционных систем должны обеспечивать документирование и протоколирование обрабатываемой в системе информации.

Доступ к данным должен быть предоставлен только авторизованным пользователям с учетом их служебных полномочий, а также с учетом категории запрашиваемой информации.

Структура базы данных должна быть организована рациональным способом, исключающим единовременную полную выгрузку информации, содержащейся в базе данных системы.

Технические средства, обеспечивающие хранение информации, должны использовать современные технологии, позволяющие обеспечить повышенную надежность хранения данных и оперативную замену оборудования.

В состав Подсистемы должна входить специализированная подсистема резервного копирования и восстановления данных.

5.3.2.2. Применение систем управления базами данных

Требования не предъявляются.

5.3.2.3. Защита данных от разрушений при авариях и сбоях в электропитании системы.

Подсистема должна обеспечивать защиту данных, находящихся на сервере БД, от разрушений при авариях и сбоях в сети электроснабжения. Источники бесперебойного питания должны обеспечивать работу серверов приложений и БД в случае скачков напряжения в сети, а в случае аварийного отключения электропитания – предоставить необходимый запас времени для запуска резервных генераторов электроэнергии или нормального завершения работы приложений и выключения оборудования.

5.3.2.4. Контроль, хранение, обновление и восстановление данных

Подсистема должна предоставлять средства для следующих операций:

- организация бесперебойного электропитания серверов;
- резервного копирования данных;

- контроля целостности хранимых данных;
- восстановления данных при их утере в случае сбоя.

5.3.3. Требования к лингвистическому обеспечению системы:

Все интерфейсы конечных пользователей Подсистемы должны быть на русском языке. Руководства и инструкции пользователей Подсистемы также должны быть на русском языке.

Инструкции и документация для сотрудников, занимающихся поддержкой, должны быть на русском языке.

Подсистема должна обеспечивать ввод и обработку данных одновременно на нескольких различных языках, использующих различные кодировки.

5.3.4. Требования к программному обеспечению системы:

5.3.4.1. Общие требования к программному обеспечению

Программное обеспечение должно быть достаточным для выполнения всех функций Подсистемы, реализуемых с применением средств вычислительной техники, а также иметь средства организации всех требуемых процессов обработки данных, позволяющие своевременно выполнять все автоматизированные функции во всех регламентированных режимах функционирования Подсистемы.

Программное обеспечение Подсистемы должно обладать следующими свойствами:

- функциональная достаточность (полнота)
- надежность (в т.ч. восстанавливаемость, наличие средств диагностики и выявления ошибок);
- адаптируемость;
- масштабируемость;
- модуль построения;
- версионность;
- удобство эксплуатации.

Программное обеспечение Подсистемы должно быть построено таким образом, чтобы отсутствие отдельных данных не сказывалось на выполнении функций Подсистемы, при реализации которых эти данные не используются.

Программное обеспечение Подсистемы должно иметь средства диагностики состояния Системы.

Подсистема должна обеспечивать защиту программного обеспечения от случайных изменений и ограничивать доступ к программному коду для конечных пользователей.

Компоненты программного обеспечения Подсистемы должны быть совместимы между собой, так и с системным программным обеспечением.

5.3.4.2. Требования к использованию типовых и поставляемых программных средств

Все используемое программное обеспечение должно быть подлинным и лицензионным.

При проектировании и разработке Подсистемы необходимо максимально

эффективным образом использовать ранее закупленное программное обеспечение.

5.3.5. Требования к техническому обеспечению:

Техническое обеспечение Подсистемы должно максимально и наиболее эффективным образом использовать существующие у Заказчика технические средства.

5.3.6. Требования к метрологическому обеспечению:

Требования не предъявляются.

5.3.7. Требования к организационному обеспечению:

5.3.7.1. Общие требования к организационному обеспечению Подсистемы

Организационное обеспечение Подсистемы должно быть достаточным для эффективного выполнения персоналом Системы возложенных на него обязанностей при осуществлении автоматизированных и связанных с ними неавтоматизированных функций с учетом их распределения по организационным уровням.

По каждой автоматизируемой функции, в т.ч. по функциям, которые выполняются во взаимодействии между Подсистемой и Системами, должны быть разработаны инструкции конечных пользователей, взаимоувязанные для всех режимов функционирования Подсистемы. Инструкции обслуживающего персонала Подсистемы должны включать указания о действиях в условиях нарушения работоспособности Подсистемы.

Подсистема должна обеспечивать автоматическую проверку на предмет ошибочности действий персонала и запрет на выполнение таких действий, в т.ч.:

- попытка внесения данных несоответствующего типа;
- попытка изменения расчетных или не редактируемых полей и пр.

5.3.7.2. Требования к структуре и функциям подразделений, участвующих в функционировании системы или обеспечивающих ее эксплуатацию

Требования не предъявляются.

5.3.8. Требования к методическому обеспечению:

В состав нормативно-правого и методического обеспечения системы должны входить следующие законодательные акты, стандарты и нормативы:

- Регламент информационного взаимодействия пользователей Системы
- Программа и методика испытаний;
- Описание Подсистемы;
- Паспорт информационной Системы;
- Матрица доступа.

6. Состав и содержание работ по созданию Системы

Работы Исполнителя по созданию Подсистемы должны включать следующие этапы и виды работ:

6.1. Стадии и этапы работ по созданию Подсистемы:

№ п/п	Состав	Содержание работ
1.	Разработка постановочных документов	Обследование Системы.
2.	Поставка программного обеспечения, оборудования, развертывание инфраструктуры	Расчет потребностей в лицензионном программном обеспечении, подготовка спецификаций программного обеспечения, требуемого для обеспечения информационной безопасности. Поставка лицензионного программного обеспечения и оборудования. Монтаж и настройка оборудования. Установка и настройка лицензионного программного обеспечения.
3.	Технорабочее проектирование	Разработка технорабочего проекта. Разработка проектных решений на отдельные виды работ.
4.	Создание программного обеспечения Подсистемы	Выполнение работ по созданию Подсистемы. Установка и настройка разработанного программного обеспечения Подсистемы.
5.	Разработка рабочей документации по Подсистеме	Разработка и согласование рабочей документации на Подсистему: − Описание Подсистемы; − Паспорт информационной Подсистемы; − Матрица доступа.
6.	Обучение пользователей и администратора Системы	Проведение занятий. Формирование протоколов обучения.
7.	Подготовка и проведение комплексных испытаний	Разработка программы и методики комплексных испытаний, подготовка комплекта тестовых сценариев. Проведение комплексных испытаний Подсистемы. Доработка программного обеспечения, актуализация рабочей документации в соответствии с результатами комплексных испытаний.
8.	Подготовка и проведение внедрения Подсистемы	Разработка плана мероприятий по внедрению Подсистемы.

		Доработка Подсистемы по результатам работ по внедрению Подсистемы. Принятие решения о вводе Подсистемы в эксплуатацию.
9.	Сопровождение Подсистемы	Выполнение работ в соответствии с гарантийными обязательствами. Послегарантийное обслуживание.

Допускается выполнять отдельные виды работ до завершения предшествующих этапов, параллельное по времени выполнение работ, включение новых этапов работ.

Сроки проведения работ должны соответствовать утвержденному календарному плану выполнения работ.

6.2. Перечень документов, по ГОСТ 34.201-89, предъявляемых по окончании соответствующих стадий и этапов работ

- Регламент информационного взаимодействия пользователей Системы – разрабатывается Исполнителем;
- Программа и методика испытаний – разрабатывается Исполнителем;
- Описание Системы – разрабатывается Исполнителем;
- Паспорт информационной Системы – разрабатывается Исполнителем.

6.3. Вид и порядок проведения экспертизы технической документации (стадия, этап, объем проверяемой документации, организация-эксперт)

- Регламент информационного взаимодействия пользователей Системы – Исполнитель осуществляет разработку документа, согласование его с руководителем проекта со стороны Заказчика, обеспечивает утверждение Регламента;
- Программа и методика испытаний - Исполнитель осуществляет разработку документа, согласование его с руководителем проекта со стороны Заказчика; обеспечивает утверждение документа;
- Описание Подсистемы - Исполнитель осуществляет разработку документа, согласование его с руководителем проекта со стороны Заказчика, обеспечивает утверждение документа;
- Паспорт информационной Подсистемы - Исполнитель осуществляет разработку документа, согласование его с руководителем проекта со стороны Заказчика, обеспечивает утверждение документа.

6.4. Программа работ, направленных на обеспечение требуемого уровня надежности разрабатываемой системы (при необходимости)

Требования не предъявляются.

6.5. Перечень работ по метрологическому обеспечению на всех стадиях создания системы с указанием их сроков выполнения и организаций-исполнителей (при необходимости)

Требования не предъявляются.

7. Порядок приемки и контроля Подсистемы

7.1. Виды, состав, объем и методы испытаний системы и ее составных частей (виды испытаний в соответствии с действующими нормами, распространяющимися на разрабатываемую систему):

Виды, состав, объем, и методы испытаний Подсистемы должны быть изложены в программе и методике испытаний Подсистемы, разрабатываемой в составе рабочей документации.

Целью проведения испытаний Подсистемы является проверка соответствия Подсистемы требованиям, изложенным в Техническом задании.

Испытания Подсистемы должны производиться на тестовом контуре. Сроки начала и продолжительность испытаний Подсистемы перед сдачей ее в эксплуатацию определяются приложением к Договору - Календарным планом работ.

7.2. Общие требования к приемке работ по стадиям (перечень участвующих предприятий и организаций, место и сроки проведения), порядок согласования и утверждения приемочной документации:

Сдача-приёмка работ производится в соответствии с Договором между Исполнителем и Заказчиком и его приложением - Календарным планом.

Основанием для сдачи-приёмки работ служит Отчёт о завершении работ, представляемый Исполнителем. Для сдачи-приемки представляется также документация, указанная в Разделе 8 настоящего Технического задания.

Для проведения сдачи-приемки выполненных работ Заказчик назначает приемочную комиссию. Приемочная комиссия осуществляет приемку работ в соответствии с требованиями настоящего Технического задания.

По результатам сдачи-приемки работ оформляется акт сдачи-приемки работ, который подписывается уполномоченным представителем Заказчика, Исполнителем.

Все создаваемые в рамках настоящей работы программные изделия (за исключением покупных программных компонент и программных компонент, разработанных Исполнителем вне рамок данного проекта) передаются Заказчику, как в виде готовых модулей, так и в виде исходных кодов, представляемых в электронной форме на стандартном машинном носителе.

Лицензии на программные компоненты, необходимые для эксплуатации разрабатываемого программного обеспечения, приобретенные Исполнителем у третьей стороны, оформляются на Заказчика.

7.3. Статус приемочной комиссии:

Статус приемочной комиссии определяется Заказчиком до проведения испытаний.

8. Требования к составу и содержанию работ по подготовке объекта автоматизации к вводу Подсистемы в действие

8.1. Приведение поступающей в Систему информации (в соответствии с требованиями к информационному и лингвистическому обеспечению) к виду, пригодному для обработки с помощью ЭВМ:

Требования не предъявляются.

8.2. Изменения, которые необходимо осуществить в объекте автоматизации:

Требования не предъявляются.

8.3. Создание условий функционирования объекта автоматизации, при которых гарантируется соответствие создаваемой Подсистемы требованиям, содержащимся в Техническом задании:

Требования не предъявляются.

8.4. Создание необходимых для функционирования Подсистемы подразделений и служб:

Требования не предъявляются.

8.5. Сроки и порядок комплектования штатов и обучения персонала:

Обучение производится в соответствии с договором между Исполнителем и Заказчиком и его приложением - Календарным планом.

9. Требования к документированию

9.1. Согласованный разработчиком и Заказчиком системы перечень подлежащих разработке комплектов и видов документов, соответствующих требованиям ГОСТ 34.201-89:

Комплект документации, созданный при разработке и внедрении Подсистемы, предоставляется Заказчику Исполнителем в печатном виде, а также на электронном носителе информации. Форматы соответствующих электронных документов должны позволять просмотр, редактирование, сохранение в редакторах Microsoft Word, Excel, Project, Visio, Adobe, ARIS.

При разработке документов должны учитываться требования действующих государственных стандартов и руководящих документов на автоматизированные системы управления и информационные технологии: ГОСТ 31.201-89, ГОСТ 34.601-90, ГОСТ 34.602-89, ГОСТ 34.603-92, РД 50-34.698-90 и т.д.

Проектная документация должна быть выпущена в объеме, необходимом для описания полной совокупности принятых проектных решений и достаточном для дальнейшего выполнения работ по созданию Подсистемы.

Разработка регламентов, стандартов, положений, инструкций должна быть выполнена с учетом действующих у Заказчика требований к оформлению нормативно-регламентирующих документов.

Сроки предоставления документов Заказчику должны соответствовать срокам завершения работ по утвержденному календарному плану выполнения подрядных работ по проекту создания и внедрения Подсистемы.

Для Подсистемы на различных стадиях создания должны быть выпущены следующие документы из числа предусмотренных в ГОСТ 34.201–89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначения документов при создании автоматизированных систем»:

- Описание технологического процесса обеспечения информационной безопасности – документ «Регламент информационного взаимодействия пользователей Системы»;
- Программа и методика испытаний - документ «Программа и методика испытаний»;
- Общее описание Подсистемы – документ «Описание Подсистемы»;
- Паспорт – документ «Паспорт информационной Подсистемы».

9.2. Требования по документированию комплектующих элементов межотраслевого применения в соответствии с требованиями ЕСКД и ЕСПД:

Требования не предъявляются.

10. Источники разработки

Государственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы. ГОСТ 34.602-89.