[ВВЕДЕНИЕ 3](#_Toc487454883)

[I Глава I. Аналитическая часть. 5](#_Toc487454884)

[1.1 Технико-экономическая характеристика предметной области и предприятия. 5](#_Toc487454885)

[1.1.1 Характеристика предприятия и его деятельности. 5](#_Toc487454886)

[1.1.2 Организационная структура управления предприятием. 11](#_Toc487454887)

[1.1.3 Программная и техническая архитектура ИС предприятия 20](#_Toc487454888)

[1.2 Характеристика комплекса задач, задачи и обоснование необходимости автоматизации 26](#_Toc487454889)

[1.2.1 Выбор комплекса задач автоматизации и характеристика существующих бизнес процессов 26](#_Toc487454890)

[1.2.2 Определение места проектируемой задачи в комплексе задач и ее описание. 27](#_Toc487454891)

[1.2.3 Обоснования необходимости использования вычислительной техники для решения задачи 30](#_Toc487454892)

[1.2.4 Анализ системы обеспечения информационной безопасности и защиты информации 33](#_Toc487454893)

[1.3 Анализ существующих разработок и выбор стратегии автоматизации «КАК ДОЛЖНО БЫТЬ» 39](#_Toc487454894)

[1.3.1 Анализ существующих разработок для автоматизации задачи 39](#_Toc487454895)

[1.3.2 Выбор и обоснование стратегии автоматизации задачи 45](#_Toc487454896)

[1.3.3 Выбор и обоснование способа приобретения ИС для автоматизации комплекса задач 47](#_Toc487454897)

[1.4 Обоснование проектных решений 49](#_Toc487454898)

[1.4.1 Обоснование проектных решений по информационному обеспечению 49](#_Toc487454899)

[1.4.2 Обоснование проектных решений по программному обеспечению 54](#_Toc487454900)

[1.4.3 Обоснование проектных решений по техническому обеспечению 57](#_Toc487454901)

[II Проектная часть 58](#_Toc487454902)

[2.1 Разработка проекта автоматизации 58](#_Toc487454903)

[2.1.1 Этапы жизненного цикла проекта автоматизации 60](#_Toc487454904)

[2.1.2 Ожидаемые риски на этапах жизненного цикла и их описание 60](#_Toc487454905)

[2.1.3 Организационно-правовые и программно-аппаратные средства обеспечения информационной безопасности и защиты информации 62](#_Toc487454906)

[2.2 Информационное обеспечение задачи 70](#_Toc487454907)

[2.2.1 Информационная модель и её описание 70](#_Toc487454908)

[2.2.2 Характеристика нормативно-справочной, входной и оперативной информации 71](#_Toc487454909)

[2.2.3 Характеристика результатной информации 72](#_Toc487454910)

[2.3 Программное обеспечение задачи 73](#_Toc487454911)

[2.3.1 Общие положения (дерево функций и сценарий диалога) 73](#_Toc487454912)

[2.3.2 Характеристика базы данных 79](#_Toc487454913)

[2.3.3 Структурная схема пакета (дерево вызова программных модулей) 91](#_Toc487454914)

[2.3.4 Описание программных модулей 91](#_Toc487454915)

[2.4 Контрольный пример реализации проекта и его описание 92](#_Toc487454916)

# ВВЕДЕНИЕ

Актуальность темы автоматизации управления видеонаблюдением между ФГБУ "ФЦТ" и ПАО "Ростелеком".

Тема автоматизации довольно обширна, но в целом она охватывает такую область как минимизация ручного труда и освобождение человека от непосредственного управления определёнными процессами.

Процесс компьютерной автоматизации начинается с появлением первой вычислительной техники и продолжается до сих пор.

В настоящее время практически во всех областях жизни используется компьютерная автоматизация. Несмотря на то, что до сих пор остаются задачи, которые не могут быть напрямую автоматизированы, тем не менее, большая часть задач вполне поддаётся управлению без участия человека.

Автоматизация даёт ощутимые преимущества:

* увеличивает скорость выполнения задачи;
* уменьшает вероятность ошибок;
* позволяет высвободить ресурсы времени сотрудников для выполнения других задач;
* гарантирует своевременность и регулярность выполнения задач;
* устраняет необходимость в рутинных ручных операциях, неизбежных при обработке информации.

Таким образом, тема автоматизации управления видеонаблюдением актуальна.

Цель дипломной работы: исследование и разработка автоматизации управления видеонаблюдением между ФГБУ "ФЦТ" и ПАО "Ростелеком".

Объект исследования: актуальная необходимость автоматизации процесса управления видеонаблюдением.

Предмет исследования: информационная система, обеспечивающая сам процесс автоматизированного управления видеонаблюдением.

Задачи, стоящие перед исследованием:

* изучение области и выявление недостатков существующей организации обработки информации;
* разработка постановки задачи;
* обоснование выбора основного проектного решения;
* разработка всех видов обеспечивающих подсистем;
* обоснование экономической эффективности проекта.

В первой главе будет дана технико-экономическая характеристика организации, представлены организационная, техническая и программные структуры организации, дана характеристика комплекса задач и обоснование необходимости автоматизации. Также первая глава затронет анализ существующих разработок и выбора стратегии автоматизации. После чего будет приведено обоснование выбранного проектного решения.

Вторая глава описывает проектную часть, в которой раскрывается содержание разработки проекта автоматизации, информационного обеспечения задачи, программного обеспечения задачи и приводится контрольный пример реализации проекта.

Третья глава содержит обоснование экономической эффективности проекта, в которой раскрывает выбор и обоснование методики расчёта и расчёт показателей экономической эффективности.

Методы исследования: анализ, синтез, моделирование, сравнение.

# Глава I. Аналитическая часть.

## Технико-экономическая характеристика предметной области и предприятия.

* + 1. Характеристика предприятия и его деятельности.

Полное название предприятия:

Федеральное государственное бюджетное учреждение «Федеральный Центр Тестирования», сокращённо ФГБУ «ФЦТ».

Цель функционирования предприятия.

Центр создан в целях содействия Рособрнадзору в осуществлении его полномочий, в том числе по организации проведения единого государственного экзамена, формированию и ведению информационных ресурсов.

Центр является некоммерческой организацией, не имеющей извлечение прибыли в качестве основной цели своей деятельности, и вправе осуществлять приносящую доход деятельность лишь постольку, поскольку это служит достижению целей, ради которых он создан, и соответствующую этим целям.

Краткая история предприятия.

Центр создан приказом Министерства образования Российской Федерации от 29 декабря 1999 г. № 1416 с наименованием государственное учреждение «Центр тестирования Министерства образования Российской Федерации». В соответствии с постановлением Правительства Российской Федерации от 17 июня 2004 г. № 288 «О Федеральном агентстве по образованию» Центр был передан в ведение Федерального агентства по образованию. Приказом Федерального агентства по образованию от 29 ноября 2004 г. № 280 государственное учреждение «Центр тестирования Министерства образования Российской Федерации» было переименовано в государственное учреждение «Федеральный центр тестирования». Распоряжением Правительства Российской Федерации от 31 декабря 2004 г. № 1749-р Центр был передан в ведение Федеральной службы по надзору в сфере образования и науки (далее - Рособрнадзор). Приказом Рособрнадзора от 5 марта 2005 г. № 472 Центр был переименован в федеральное государственное учреждение «Федеральный центр тестирования». Приказом Рособрнадзора от 21 апреля 2011 г. № 1021 Центр был переименован в федеральное государственное бюджетное учреждение «Федеральный центр тестирования».

Направления деятельности предприятия.

а). Информационно-технологическое обеспечение управления системой образования:

• тиражирование и доставка экзаменационных материалов для проведения государственной итоговой аттестации по образовательным программам среднего общего образования в форме единого государственного экзамена (ЕГЭ) в субъекты Российской Федерации и российские образовательные организации, расположенные за пределами территории Российской Федерации, дипломатические представительства и консульские учреждения Российской Федерации, представительства Российской Федерации при международных (межгосударственных, межправительственных) организациях (ЗОО);

• подготовка и организация проведения государственной итоговой аттестации по образовательным программам основного общего и среднего общего образования в ЗОО, в том числе технологическое сопровождение процедуры проведения итогового сочинения (изложения);

• формирование статистической информации о подготовке и проведении государственной итоговой аттестации по образовательным программам основного общего и среднего общего образования.

б). Методическое обеспечение образовательной деятельности:

• консультирование по вопросам подготовки и проведения государственной итоговой аттестации по образовательным программам среднего общего образования органов исполнительной власти 85 субъектов Российской Федерации, осуществляющих государственное управление в сфере образования, учредителей образовательных организаций, расположенных за пределами территории Российской Федерации и реализующих имеющие государственную аккредитацию образовательные программы среднего общего образования, и загранучреждения Министерства иностранных дел Российской Федерации, имеющие в своей структуре специализированные структурные образовательные подразделения, в том числе с использованием видеотрансляций.

в). Создание и развитие информационных систем и компонентов информационно-телекоммуникационной инфраструктуры:

• развитие федеральной информационной системы обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования, и приема граждан в образовательные организации для получения среднего профессионального и высшего образования (ФИС ГИА и Приема) как в целом, так и отдельных подсистем и компонентов;

• развитие программных средств региональных информационных систем обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования;

• развитие инфраструктуры информационно-коммуникационных технологий, необходимой для эксплуатации ФИС ГИА и Приема;

• развитие комплексной системы защиты информации объекта информатизации ФГБУ "ФЦТ".

г). Техническое сопровождение и эксплуатация, вывод из эксплуатации информационных систем и компонентов информационно-телекоммуникационной инфраструктуры:

• организационно-техническое обеспечение формирования и ведения ФИС ГИА и Приема;

• обеспечение информационной безопасности Рособрнадзора;

• техническое сопровождение защищенных сетей передачи данных и подключение к защищенным сетям передачи данных региональных центров обработки информации субъектов Российской Федерации, организаций осуществляющих образовательную деятельность для внесения соответствующих сведений в ФИС ГИА и Приема.

д). Осуществление функций Удостоверяющего центра

ФГБУ «ФЦТ» также осуществляет следующие приносящие доход виды деятельности:

• информационно-методическое и организационно-технологическое обеспечение проведения ГИА и иных форм оценки качества образования;

• разработка, использование и распространение методов, алгоритмов баз данных и программ для ЭВМ по подготовке, проведению и обработке результатов тестирования с целью оценки качества образования; обеспечение информационной безопасности вычислительных систем и сетей;

• проведение экспертизы процедур оценки качества образования в рамках проверок качества образования в образовательных организациях.

Таблица 1.1.

Основные характеристики (показатели эффективности) видов деятельности

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № | Основные | 2015 | 2016 | Отклонения |
| п/п | показатели | год | год | (%)2015 к |
|  |  |  |  | 2016 |
| 1. | Объём предоставленных услуг, тыс. руб. | 572927 | 429138 | 74 |
| 2. | Себестоимость предоставленных услуг, тыс. руб. | 493340 | 344757 | 70 |
| 3. | Затраты на 1 рубль  предоставленных  услуг, коп | 0,86 | 0,8 | 93 |
| 4. | Прибыль, тыс. руб. | 79587 | 84381 | 106 |
| 5. | Рентабельность, % | 14 | 20 | 142 |
| 6. | Численность персонала, чел; | 110 | 120 | 109 |
| 7. | Производительность труда, тыс. руб./ чел | 5208 | 3576 | 70 |
| 8. | Среднемесячная заработная плата,  руб. | 30000 | 45000 | 150 |
| 9. | Фонд оплаты труда,  руб. | 87645 | 113728 | 130 |

* + 1. Организационная структура управления предприятием.

На рис. 1.1 изображена существующая организационная схема управления предприятием.



Рисунок 1.1. Организационная структура ФГБУ «ФЦТ».

Непосредственное руководство деятельностью Центра осуществляется его директором на принципах единоначалия. Директору подчиняются заместители директора, которые управляют отделам и несут ответственность за соответствующие их направлению задачи. Сотрудники отделов подчиняются начальникам соответствующих отделов. Начальники отделов занимаются постановкой задач и контролируют их выполнение.

Директор в соответствии с законодательством Российской Федерации и Уставом организации:

а). Организует финансово-хозяйственную деятельность Центра;

б). Без доверенности действует от имени Центра и представляет Центр в отношениях со всеми юридическими и физическими лицами, включая органы государственной власти и местного самоуправления;

в). Управляет имуществом Центра в порядке, установленном законодательством Российской Федерации и настоящим Уставом;

г). Заключает и расторгает трудовые договоры с работниками Центра в соответствии с трудовым законодательством Российской Федерации, распределяет обязанности между ними, определяя их полномочия;

д). Заключает договоры, гражданско-правовые договоры, государственные контракты и иные соглашения;

е). Выдает доверенности, открывает и закрывает счета в банках;

ж). Издает приказы, распоряжения, дает указания, обязательные для работников Центра;

з). Применяет к работникам Центра меры поощрения и дисциплинарные взыскания;

и). Утверждает структуру и штатное расписание Центра, планы работы Центра и его подразделений, распределяет между ними объем работ, финансовые и материально-технические ресурсы;

к). Утверждает должностные обязанности и планы работы заместителей директора Центра, должностные обязанности работников Центра в соответствии с трудовым законодательством Российской Федерации и штатным расписанием Центра;

л). Представляет на утверждение в Рособрнадзор план финансово­ хозяйственной деятельности;

м). По согласованию с Рособрнадзором вправе выступать с сообщениями по вопросам деятельности Центра, осуществляемым по поручению Рособрнадзора или входящим в компетенцию Рособрнадзора;

н). Устанавливает работникам Центра размеры надбавок, доплат и премий за счет средств Центра, полученных от приносящей доходы деятельности, принимает решения по другим вопросам деятельности Центра;

о). Определяет самостоятельно или поручает созданной им комиссии определять характер и объем сведений, составляющих служебную и коммерческую тайну, по согласованию с Рособрнадзором;

п). Несет ответственность за сохранность документов, образующихся в его деятельности (управленческих, финансово-хозяйственных, по личному составу и др.), и в случае ликвидации обеспечивает передачу в установленном порядке архивных документов на государственное хранение.

Заместитель директора подчиняется напрямую директору.

В должностные обязанности входит:

а). Управление деятельностью подчинённых отделов.

б). Постановка задач начальникам подчинённых отделов и контроль их исполнения.

Отдел управления ИТ-инфраструктурой и эксплуатации информационных систем, основные задачи:

* Организация функционирования единого информационного пространства организации посредством реализации комплекса организационных, методических и технических мероприятий, с помощью методов и средств информационно-коммуникационных технологий;
* Координация и регулирование деятельности ИT-комплекса (за исключением вопросов информационной безопасности);
* Анализ потребности закупаемого оборудования (технические характеристики, основные параметры и возможности), соответствия конфигурации поставленным задачам, а также подготовка и сопровождение технического задания.

Отдел программного обеспечения, основные задачи:

* Осуществляет разработку технических проектов ПО, построение архитектуры программных систем, определение технических и программных требований к ПО;
* Проводит анализ поступающей информации о сбоях в работе ПО, связанных с ошибками в ПО и принимает меры к их оперативному устранению;
* Оказывает консультативную помощь отделу внедрения по вопросам функционирования используемого программного обеспечения и используемым технологиям;
* Согласно получаемым из отдела внедрения техническим заданиям, осуществляет доработку и разработку нового ПО, связанного с решением вопросов социальной защиты населения, электронного информационного межведомственного взаимодействия;
* Осуществляет разработку новых версий ПО;
* Осуществляет предварительное тестирование новых версий ПО на правильность реализации алгоритмов и соответствие техническому заданию.

Информационно-аналитический отдел, основные задачи:

* составление планов, статистических и аналитических отчетов;
* подготовка докладов, иных информационно-аналитических материалов.

Отдел перспективных разработок, основные задачи:

* Поиск и выявление перспективных разработок в научно-технической сфере, организация проведения исследований, содействие в оформление в проекты и их реализации;
* Формирование коммерческой политики организации в инновационной и научно-технической деятельности;
* Проведение исследований, направленных на формирование долгосрочных планов развития инновационных направлений в научно-технической сфере организации.

Отдел проектирования информационных систем, основные задачи:

* Анализ и изучение проблем обслуживания информационных систем;
* Участие в составлении технических заданий по созданию информационных систем;
* Подготовка планов проектирования и внедрения информационных систем и контроль за их выполнением;
* Разработка и проектирование схем обработки информации по всем задачам информационных систем и технологических процессов обработки информации при помощи средств вычислительной техники;

Финансово-экономический отдел, основные задачи:

* Реализация финансовой стратегии и финансовой политики организации;
* Организация финансовой деятельности с целью эффективного использования финансовых ресурсов;
* Разработка прогнозов экономического развития организации и участие в формировании ключевых показателей деятельности.
* Участие в разработке бизнес-планов, составление перспективных и текущих финансовых планов, и бюджетов организации и оперативный контроль их выполнения;
* Предоставление необходимой финансовой оперативной, регулярной и аналитической информации внутренним и внешним пользователям;
* Комплексный экономический и финансовый анализ деятельности организации, разработка мероприятий по повышению эффективности управления финансами, снижению финансовых рисков и увеличению прибыльности организации;
* Контроль над соблюдением финансовой дисциплины, своевременным и полным выполнением договорных обязательств, расходами и поступлением доходов.

Методический отдел, основные задачи:

* Нормативно регламентирующее обеспечение деятельности организации;
* Организация работы по изучению новых государственных образовательных стандартов, разработка на их основе методической документации по проведению экзаменов.

Отдел по работе с регионами, основные задачи:

* Координация деятельности и организация эффективного взаимодействия организации с общественными организациями и органами власти с соответствующими региональными структурами.

Отдел закупок, основные задачи:

* Определение потребности в материальных ресурсах;
* Поиск, анализ данных, выбор поставщиков;
* Заключение договоров и контроль исполнения;

Отдел юридического обеспечения и кадрового учета, основные задачи:

* Правовое обеспечение деятельности организации и её структурных подразделений, оказание правовой поддержки в выполнении стоящих перед ними задач;
* Организация и ведение договорно-правовой работы;
* Подготовка локальных актов организации;
* Взыскание задолженности, претензионная работа, защита интересов организации в суде.
* Контроль соблюдения организации и её работниками требований нормативно-правовых актов;
* Комплектование организации кадрами персонала в соответствии с целями, стратегией и профилем организации, изменяющимися внешними и внутренними условиями её деятельности;
* Разработка кадровой политики и стратегии организации;
* Подбор, отбор и расстановка кадров на основе оценки их квалификации, личных и деловых качеств;
* Контроль правильности использования труда работников организации;
* Обеспечение трудовых прав, льгот и гарантий работников организации;
* Документационное и архивное обеспечение деятельности организации.

Отдел информационной безопасности, основные задачи:

* Разработка единой политики (концепции) обеспечения информационной безопасности организации, определение требований к системе защиты информации организации и документообороту на бумажных и электронных носителях;
* Организация мероприятий и координация работ всех подразделений по комплексной защите информации на всех этапах технологических циклов ее создания, переноса на носитель (бумажный или электронный), обработки и передачи в соответствии с единой политикой обеспечения информационной безопасности организации;
* Контроль и оценка эффективности принятых мер и применяемых средств защиты информации.

Отдел технической защиты информации, основные задачи:

* Разработка проектов перспективных и текущих планов работ по защите информации, составление отчетов об их выполнении;
* Соблюдение режима проводимых работ и сохранение конфиденциальности документированной информации;
* Проведение работ по организации, координации, методическому руководству и контролю их выполнения по вопросам защиты информации и разработка технических средств контроля.
* Работа по заключению договоров на выполнение работы по защите информации, обеспечение финансирования работ, в том числе выполняемых по договорам;
* Разработка технических заданий по созданию безопасных информационных технологий, отвечающих требованиям комплексной защиты информации.

Административно-хозяйственный отдел, основные задачи:

* Административно-хозяйственное обеспечение деятельности организации: техническое обслуживание зданий, помещений, оборудования (лифтов, систем отопления, водоснабжения, вентиляции, электросетей и т.д.), планирование, организация и контроль проведения их текущих и капитальных ремонтов, снабжение мебелью, хозяйственным инвентарем, средствами механизации инженерного и управленческого труда, организация транспортного обеспечения и охраны;
* Организационно-методическое руководство и контроль деятельности структурных подразделений организации по вопросам хозяйственного обслуживания, рационального использования материальных и финансовых ресурсов, сохранности собственности организации;
* Подготовка и представление руководству информационно-аналитических материалов о состоянии и перспективах развития хозяйственного обеспечения деятельности организации, разработка предложений по совершенствованию службы отдела;
* Совершенствование и внедрение новых методов организации работы, в том числе на основе использования современных информационных технологий;
* Участие в подготовке и исполнении управленческих решений руководства по вопросам административно-хозяйственного обеспечения деятельности организации.
  + 1. Программная и техническая архитектура ИС предприятия

На рисунке 1.2 приведена техническая архитектура ФГБУ «ФЦТ».

Рисунок 1.2. Техническая архитектура ФГБУ «ФЦТ».

Техническая структура представляет собой два контура – защищённый и открытый.

Связь с базами регионального уровня осуществляется посредством выделенных каналов доступа. Данные репликации приходят по выделенным каналам доступа на брандмауэр CISCO ASA5510, после чего отправляются на маршрутизатор Brocade FCX648S.

В открытый контур входят клиентские машины (АРМ), сервер открытой сети, имеющий сетевое хранилище, а также выход в сеть Интернет через аппаратный брандмауэр CISCO ASC.

Программная структура представляет собой также двухконтурную систему.

Закрытый контур имеет подсистемы серверной виртуализации VMware, обеспечивающие защищённый доступ извне.

Для организации внутреннего контура защиты используется сетевая система Infotecs ViPNet.

Рабочая станция сотрудника имеет RDP View Client, который посредством протоколов HTTPS/PCoIP позволяет совершить соединение с Secure GW сервер-шлюзом, который, в свою очередь, позволяет установить RDP сеанс с VMware Agent на сервере защищённой сети.

Защищённый контур представляет собой мощный и защищённый сервер, работающий под управлением ОС Windows Server 2008 и обеспечивающий работу базы федерального уровня (ФБД «MAINDB») на основе MS SQL Server 2012, для которой настроена репликация с базами регионального уровня (РБД) с MS SQL версий от 2008 до 2012.

Открытый контур представляет собой соединение по протоколу TCP/IP с сервером в открытой(незащищённой) сети, который имеет доступ в интернет посредством протокола HTTPS или HTTP.

Хранение данных осуществляется посредством LDAP Windows 2008 сервера незащищённой сети, который имеет возможность безопасно обращаться как к Raid массивам защищённой сети, так и к сетевым хранилищам данных открытой сети.

Характеристики персональных компьютеров приведены в Таблице 1.2.

Таблица 1.2.

Характеристики персональных компьютеров автоматизированных рабочих мест

|  |  |  |
| --- | --- | --- |
| № | Описание | Характеристики |
| п/п |
|  |
| 1. | Модель | ProDesk 600 G1 Tower |
| 2. | Процессор компьютера | Intel Core i5-4570 |
| 3. | Видео | Intel HD Graphics 4600 |
| 4. | Аудио | Встроенная звуковая карта Realtek ALC221 |
| 5. | Оперативная память | DDR3 4 ГБ (1 x 4 ГБ; 4 слота DIMM) |
| 6. | Объем накопителя компьютера | 500 Гб HDD |
| 7. | Сеть | 10/100/1000 Мбит/сек Intel I217LM |
| 8. | Разъемы компьютера | 2 x USB 3.0, 4 x USB 2.0, VGA (15-pin D-SUB), RJ-45, 2 x PS/2, COM, Линейный вход, Линейный выход, 2 x DisplayPort |
| 9. | Безопасность | Включение/отключение последовательного, параллельного и USB-портов (в BIOS), отключение портов SATA (в BIOS), пароль на BIOS, пароль для администрирования, электромагнитный замок и датчик защелки крышки |

Таблица 1.3.

Характеристики серверов

|  |  |  |
| --- | --- | --- |
| № | Описание | Характеристики |
| п/п |
|  |
| 1. | Сервер открытой сети | 4 x Intel Xeon E7-8890 v3  16 x 16GB DDR4-1866 ECC Reg.  Smart Array P830i 12G 4GB FBWC  5 (up to 10) SFF 2.5" HotPlug bays  SAS/SATA HDD/SSD optional  2 x 10 Gb Ethernet  DVD not available  4 x 1500W HS PS  HP OneView Advanced |
| 2. | Сервер защищённой сети | 4 x Intel Xeon E7-4850 v3  8 x 16GB DDR4-1866 ECC Reg.  Smart Array P830i 12G 4GB FBWC  5 (up to 10) SFF 2.5" HotPlug bays  SAS/SATA HDD/SSD optional  2 x 10 Gb Ethernet  DVD not available  4 x 1200W HS PS  HP OneView Advanced |

На рисунке 1.3 приведена программная архитектура ФГБУ «ФЦТ».



Рисунок 1.3. Программная архитектура ФГБУ «ФЦТ».

## Характеристика комплекса задач, задачи и обоснование необходимости автоматизации

* + 1. Выбор комплекса задач автоматизации и характеристика существующих бизнес процессов

Партнёром организации ФГБУ «ФЦТ» является компания ПАО «Ростелеком», которая занимается техническим обеспечением и проведением видеонаблюдения в аудиториях в периоды сдачи ГИА.

Управление видеонаблюдением фактически состоит из передачи данных в ПАО «Ростелеком» об аудиториях, участвующих в проведении экзаменов на конкретные даты в конкретных регионах.

До внедрения автоматизации, передача информации о включаемых аудиториях производилась вручную: отдел по работе с регионами (см. Рис. 1.1) собирал данные из регионов, получая от них списки аудиторий на конкретные даты. Далее, списки их регионов компилировались сотрудниками отдела в сводный список, который направлялся начальнику отдела, а далее отправлялся начальником отдела по электронной почте в ПАО «Ростелеком».

Данная схема задействовала большое количество сотрудников, и, фактически была очень слабо автоматизирована. Со стороны региональных центров обработки информации были задействованы сотрудники, которые готовят списки аудиторий. На федеральном уровне были задействованы кураторы регионов, которым стекалась информация об аудиториях, участвующих в видеонаблюдении. Начальник отдела по работе с регионами должен был скомпилировать финальный список единым документом. Большое количество сотрудников, вовлечённых в процесс сбора и отправки информации способствовало появлению большому количеству неточностей или явных ошибок. Также это занимало большое количество времени.

* + 1. Определение места проектируемой задачи в комплексе задач и ее описание.

На схеме 1.4 приведена бизнес-модель деятельности ФГБУ «ФЦТ».



Рисунок 1.4 Функциональная модель ФГБУ «ФЦТ».

На схеме 1.5 приведена схема IDEF0 обработка данных тестирования.



Рисунок 1.5 Декомпозиция модели обработки данных тестирования.

Из всего комплекса задач по автоматизации получения данных от регионов мной будет исследоваться задача по автоматизации передачи данных от регионов в ПАО «Ростелеком» для организации видеонаблюдения.

Входные информационные потоки можно представить в следующем виде:

* Сериализованные данные из БД.
* Расписание выгрузки в сериализованном виде, созданное оператором.

Выходные информационные потоки можно представить в следующем виде:

* Изменения, отправленные на исходящий сервер в системе контроля версий.

Процесс, которые происходит при передаче данных: Пользователь формирует расписание для отправки данных, сервис открытой сети работает по заданному расписанию, сервис защищённой сети работает регулярно с наперёд заданным интервалом.

Причиной выбора для исследования именно этой задачи, стало моё участие в выгрузке данных для видеонаблюдения, в ходе которого было выявлено полное отсутствие автоматизации процесса управления видеонаблюдением.

Задачи по автоматизации выгрузок из базы данных возникают постоянно.

Данные требуются различным отделам организации. Регулярные выгрузки данных требуются информационно-аналитическому отделу в виде регулярно формируемой статистики. Выгрузка данных по требованию или по заданному календарному режиму также необходимы в работе отделов информационной безопасности и отделу перспективных разработок.

В настоящий момент, автоматизация видеонаблюдением требует большого количества специалистов, занятых кропотливым рутинным трудом.

Задействован весь отдел по работе с регионами включая начальника отдела.

Задействован специалист по работе над видеонаблюдением со стороны ПАО «Ростелеком».

Решение, которое разработано мной, не требует такого количества специалистов для сбора данных. Сбор, компиляция и передача данных происходит в автоматизированном режиме, где пользователю требуется только задать режим отправки изменений.

Фактически, после реализации данной работы, управлять регулярностью видеонаблюдения может любой сотрудник с надлежащими правами доступа и после знакомства с инструкцией по использованию.

* + 1. Обоснования необходимости использования вычислительной техники для решения задачи

Схема документооборота приведена на таблице 1.1.

Таблица 1.1

Схема документооборота ФГБУ «ФЦТ» при существующей организации процесса управления видеонаблюдением.

|  |  |  |  |
| --- | --- | --- | --- |
| Исполнитель  Действие | Зам. директора | Отдел по работе с регионами | Бухгалтерия |
| 1. Заказ на получение данных видеонаблюдения. | Заявка на поставку данных |  |  |
| 2. Сбор данных видеонаблюдения. |  | Отчёт по региону |  |
| 3. Компиляция и отправка данных видеонаблюдения. |  | Сводный отчёт по регионам | Акт поставки данных |

Оценка трудозатрат приведена в таблице 1.2.

Таблица 1.2

Характеристики систем автоматизации синхронизации данных.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № | Наименование операции | Кол-во строк в документе | Кол-во операций в год | Объём работы в год(строк) | Трудозатраты в год (час) |
| п/п |
| 1. | Заявка на поставку данных | 80 | 51 | 4080 | 80 в час = 51 |
| 2. | Отчёт по региону | 200 | 51 | 10200 | 100 в час = 102 |
| 3. | Сводный отчёт по регионам | 17200 | 51 | 877200 | 100 в час = 8772 |
| 4. | Акт поставки данных | 100 | 51 | 5100 | 100 в час = 51 |
| ИТОГО | | | | | 8976 |

Использование вычислительной техники при решении комплекса задач, описываемого в данной работе, обуславливается рядом факторов. Объем и качество выходной информации не позволит решать задачи без использования вычислительной техники быстро и, что важно, корректно. Необходимость постоянной связи с различными юридическими базами данных, возможность использования локальной вычислительной сети, средств телекоммуникации - другие факторы, определяющие методы решения поставленных задач с использование вычислительной техники.

При этом требуется учитывать следующие требования:

- обеспечение достоверности обрабатываемой информации;

- решение задач в установленные сроки;

- обеспечение минимальных трудовых и стоимостных затрат на обработку данных;

- наличие возможности обработки данных на ЭВМ;

- возможность решения задачи в различных режимах.

Эти требования могут быть выполнены за счет нескольких факторов:

- сокращение числа операций, особенно ручных;

- разработка системы жесткого контроля вводимой информации;

- снижение объема обрабатываемых данных (ведение НСИ);

- повышение квалификации пользователей, улучшение условий труда и, как следствие, повышение производительности.

На выбор способа сбора, регистрации и передачи данных влияют следующие факторы:

- удаленность источников информации от центра обработки данных;

- возможность связи с источниками информации по выделенным каналам связи.

Кроме того, необходимо учесть, что базовая технология была ручная. Она имела множество недостатков:

— низкая производительность труда из-за большого числа вычислений

— большая трудоемкость

— необходимость привлечения большого числа сотрудников для решения всего комплекса задач

— низкая оперативность

— несовершенство организации сбора и регистрации информации

— недостоверность получаемых результатов

Кроме этого, постоянно нарастающие потоки информации и постоянное усложнение технологии расчетов и необходимость проведения по ним динамического анализа в ближайшей перспективе сделали бы ручной вариант просто нереальным.

С внедрением автоматизированной технологии расчетов, сбора и регистрации большинство из перечисленных недостатков были устранены и появились новые возможности в проведении анализа. Основные преимущества, достигнутые после внедрения машинного варианта:

— появилась возможность проведения более сложных расчетов в динамике

— появилась возможность проведения различных форм анализа данных

— практически полная независимость от объемов и сложности расчета

— разделение труда и разделение функций по рабочим местам и сотрудникам

— более оперативная обработка данных

* + 1. Анализ системы обеспечения информационной безопасности и защиты информации

В организации ФГБУ «ФЦТ» существует своя политика безопасности. Каждый сотрудник при поступлении получает должностную инструкцию, в которой четко описаны его права и обязанности с точки зрения информационной безопасности. Каждому сотруднику присваивается логин в систему Доменной авторизации, в рамках которой выдается доступ к определенным ресурсам сети и доступа в глобальную сеть интернет. Для данной учетной записи есть пароль, а у пароля есть своя политика безопасности, которая регламентирует срок действия пароля и его криптографическую стойкость В большинстве случаев количество входящего трафика не ограничивается, зато ограничивается список разрешённых сайтов. Для получения доступа к закрытым сайтам следует написать заявку на горячую линии с приложенным одобрением руководителя отдела. Далее эта заявка будет согласована на уровне службы Безопасности организации и только после этого доступ будет предоставлен или не предоставлен с указанием причин.

В организации реализована своя политика защиты информации: на уровне человеческого фактора и программным образом. Аппаратного ограничения нет.

В отделе Информационной Безопасности есть определённая должность по ИБ, через данного сотрудника согласовывается доступ к определенным ресурсам и только потом заявка подаётся на сетевых администраторов.

В рамках отдельной структуры Службы безопасности, которая контролирует уровни доступа по проксимити картам (пропуска) считывание датчиков тревоги и просматривает видеонаблюдение есть отдельный человек в данной структуре, который занимается именно Информационной безопасностью. Все заявки по доступу к ресурсам и подключению.

Защита информации в серверной регламентируется следующими ограничениями доступа:

1) Права доступа по электронному пропуску (проксимити - карта);

2) Роспись за получение и сдача ключа у охранника;

3)Разблокировка датчиков открытия двери у оперативного дежурного ИБ.

Средства защиты от инсайдерских угроз в организации, следующие:

За каждым пользователем закреплён компьютер и монитор, которые имеют инвентарный номер, за который он несёт материальную ответственность.

Физически – сеть состоит из двух доменов, которые имеют общий шлюз.

Вход на компьютеры и серверы в защищённой сети происходит через защищённую сеть VipNet.

Технически - защита информации осуществляется при помощи системы паролей для доступа к ресурсам информационной системы разного уровня. Прежде всего, это пароль входа пользователя в операционную систему его рабочего места. Ввод этого пароля открывает пользователю доступ к ресурсам данного компьютера и к документам, хранящимся на нем. При этом политика безопасности должна быть настроена таким образом, чтобы пользователь не был полным «хозяином» на своем рабочем месте и не мог, например, установить вредоносное программное обеспечение или программы по копированию информации. Ограничение прав несколько осложняет работу пользователей, но при этом даёт гарантию защищенности данных. Необходимо всегда находить баланс между удобством и комфортом работы пользователя и безопасностью хранения корпоративной информации или информации о клиентах.

Когда пользователь вводит свой пароль входа в операционную систему, он получает доступ не только к ресурсам данного компьютера, но и к ресурсам компьютерной сети организации. Это возможно в том случае, если пользователь входит на компьютер как доменный или сетевой пользователь. В этом случае отнестись к разграничению прав пользователей в сети нужно еще более внимательно. Настроить права сетевого пользователя нужно таким образом, чтобы дать ему возможность беспрепятственно работать со своими документами, но при этом ограничить доступ к документам, прав на работу с которыми у него нет, либо это только права на просмотр. В этом случае решается одновременно задача защиты данных от несанкционированного доступа и от случайной их порчи.

Прерогативой распределения прав пользователей обладает на предприятии системный администратор. Именно он должен разграничить права пользователей по доступу к документам и приложениям как в сети, так и на локальных компьютерах.

Отдельным уровнем защиты информации является парольная защита на вход в сеть защищённого контура через систему VipNet.

ViPNet Administrator — программный комплекс, предназначенный для настройки и управления защищенной сетью, включающий в себя:

* ViPNet NCC (Центр управления сетью, ЦУС) — приложение для конфигурирования и управления виртуальной защищенной сетью ViPNet.
* ViPNet KCA (Удостоверяющий и ключевой центр, УКЦ) — приложение, которое выполняет функции центра формирования ключей шифрования и персональных ключей пользователей.
* Функции Удостоверяющего центра — издание серти­фикатов для аутентификации, электронной подписи, шифрования и других криптографических операций.
* Криптографические алгоритмы зависят от используемого криптопровайдера в данном случае это ViPNet CSP.

В результате доступ гибко настраивается только к нужным данным в информационной системе, скрыв от несанкционированного доступа и от возможности случайной порчи данные, доступа к которым у определённого круга пользователей нет.

Ещё одним уровнем парольной защиты информации является пароль доступа к базе данных SQL Server. Данные, хранящиеся в базе данных защищены не только системой разграничения прав доступа домена сети, но и системой SQL Server, что на порядок повышает уровень безопасности работы.

Для защиты ЛВС и компьютеров от внешних угроз используется пакет Kaspersky Enterprise Space Security, который выполняет следующие функции:

* Защита от хакерских атак. Современные хакеры используют для атак кейлоггеры (клавиатурные шпионы) и руткиты — программы, которые позволяют получить несанкционированный доступ к данным и при этом избежать обнаружения. Антивирусное ядро эффективно нейтрализует эти угрозы, предотвращая несанкционированный доступ к компьютерам корпоративной сети.
* Фишинг. Также существует защита от фишинга. База URL-адресов фишинговых сайтов постоянно пополняется; с её помощью распознаются и блокируются подозрительные ссылки, а также фильтруются фишинговые электронные сообщения, повышая общий уровень защиты ЛВС.
* Сетевой экран. Kaspersky Enterprise Space Security имеет сетевой экран нового поколения, а также встроенную в него систему обнаружения и предотвращения вторжений, обеспечивают защиту пользователей при работе в сети.
* Фильтрация электронной почты. Посредством фильтрации осуществляется безопасная работа с электронной почтой. Весь поток почтовых сообщений сканируется на уровне протоколов передачи данных (POP3, IMAP, MAPI и NNTP для входящей почты и SMTP для исходящей), включая SSL-соединения. Сканируются в том числе файлы и ссылки, передаваемые через программы мгновенного обмена сообщениями (ICQ, MSN и др.). Проверка почтовых сообщений осуществляется в режиме реального времени. Зараженные объекты подвергаются лечению или удаляются.
* Контроль использования съемных устройств. Вредоносные программы могут проникнуть на компьютеры корпоративной сети через USB-носители, а также внешние устройства ввода/вывода и хранения данных. Kaspersky Enterprise Space Security позволяет проводить антивирусную проверку таких устройств и контролировать их использование, предотвращая заражение сети.
* Защита от массовых спам-рассылок. В приложении для защиты почты, входящем в состав Kaspersky Enterprise Space Security, реализованы передовые технологии эвристического и лингвистического анализа сообщений, а также эффективные методы выявления спама, поступающего в виде изображений. Kaspersky Enterprise Space Security также поддерживает работу с системой мгновенного обнаружения угроз (UDS), содержащей сведения о новейших угрозах, обновляемые в режиме реального времени. Это позволяет отфильтровывать более 99% нежелательных электронных сообщений.

## Анализ существующих разработок и выбор стратегии автоматизации «КАК ДОЛЖНО БЫТЬ»

* + 1. Анализ существующих разработок для автоматизации задачи

На рынке существует много решений, которые могут обеспечивать требуемый функционал в задаче синхронизации данных.

Одним из доступных проприетарных решений является продукция фирмы «SiteDesigner Technologies, Inc.», программный комплекс «BatchSync Secure».

BatchSync Secure - это высокоскоростное и безопасное решение для автоматизации синхронизации файлов, копирования, перемещения, зеркалирования, репликации и резервного копирования по FTP, FTP / S через SSL / TLS и SFTP через SSH2-соединения. BatchSync Secure предназначен для запуска как запланированных задач, так непосредственных задач на сервере с расширенными параметрами ведения журнала и уведомлениями по электронной почте, которые помогут в удаленном мониторинге.

Основными возможностями «BatchSync Secure» являются.

* Сохранение источника синхронизации и целевых папок - с параметрами - в качестве задачи синхронизации;
* Запуск задач синхронизации одним щелчком мыши;
* Sync Preview - просмотр файлов, которые будут переданы в древовидной структуре, без фактической передачи;
* SyncDB автоматически отслеживает изменения файлов;
* Многопоточные передачи для ускорения синхронизации;
* Сжатие файлов «на лету» для ускорения передачи;
* Односторонняя и двухсторонняя синхронизация;
* Рекурсивная синхронизация папок и их подпапок (можно исключить подпапки с фильтрами);
* Фильтровать файлы для включения по имени файла / папке, размеру, дате изменения и атрибутам;
* Фильтровать файлы для исключения по имени файла / папки, размеру, дате изменения и атрибутам;
* Настройка правил для обработки конфликтов (тот же файл был изменен как для источника, так и для адресата);
* Автоматическое возобновление прерванных передач;
* Автоматическое повторное подключение и возобновление неограниченного количества раз (пользовательские максимальные повторы, таймауты и т. д.);
* Необязательно удалять файлы по месту назначения, которых нет в источнике;
* Расширенные параметры ведения журнала с автоматическими схемами копирования журналов;
* Синхронизация локальных, сетевых и FTP-папок.

Ещё одним решением является программный комплекс «SymmetricDS», который разрабатывается как открытый проект компанией разработчиков «JumpMind».

«SymmetricDS» - это программное обеспечение с открытым исходным кодом для репликации базы данных с поддержкой односторонней репликации, репликации с несколькими ведущими устройствами, фильтрованной синхронизацией и преобразованиями. Используя технологии Интернета и баз данных, он может реплицировать данные асинхронно, как запланированные или почти в режиме реального времени. Разработанный для масштабирования до большого количества баз данных и работы между различными платформами, он работает через соединения с низкой пропускной способностью и может выдерживать периоды отключения сети.

Основные достоинства комплекса «SymmetricDS».

* Кроссплатформенность. Работает на большинстве операционных систем, включая мобильные устройства, и может синхронизировать любую базу данных с любой поддерживаемой базой данных;
* Многопоточность - многопоточная архитектура извлекает, передает и загружает данные параллельно;
* Работа с каналами - таблицы сгруппированы в независимые каналы, у которых есть собственная очередь потоков для синхронизации;
* Автоматическое восстановление. Патчи с ошибкой повторяются до тех пор, пока они не добьются успеха, поэтому синхронизация может восстановиться после сбоя сети;
* Транзакционная безопасность - изменения данных записываются и воспроизводятся в том же порядке и в пределах одной транзакции;
* Мульти-мастер - та же таблица может быть синхронизирована как с хост-системой, так и с нее, избегая циклов обновления;
* Трансформация - фильтрация, подмножество и преобразование данных во время фазы извлечения или загрузки;
* Обнаружение конфликтов. Обнаружение конфликтов и автоматическое их устранение во время синхронизации с несколькими мастерами;
* Схема таблицы - опциональное создание и обновление схемы базы данных;
* Предварительная загрузка данных;
* Центральная конфигурация - вся конфигурация получена от центрального сервера регистрации и хранится в синхронизации;
* Несколько вариантов развёртывания - развертывание с использованием автономного движка, веб-приложения (WAR) или встроенного в приложение;
* Эффективный протокол - быстрый потоковый формат данных, который легко генерировать, анализировать и загружать. Транспорт также сжимается по умолчанию;
* Мониторинг. Мониторы отслеживают проблемы, такие как пакетные ошибки или отставания, и отправляют уведомление по электронной почте;
* Удаленное управление. Управление через инструменты командной строки и консоль управления;
* Расширяемость - добавление настроек через расширения и плагины.

Также можно рассмотреть проприетарную разработку ApexSQL Data Diff – инструмент SQL Server для поиска различий в данных и синхронизации их между собой. Этот инструмент позволяет находить различия не только между базами данных, но и анализировать резервные копии БД, как обычные, так и сжатые. В результате анализа можно получить подробный отчёт о найденных расхождениях и файл синхронизации, который можно выполнить.

Ключевые возможности:

* Синхронизация БД из различных источников;
* Восстановление данных из удалённой таблицы без наличия резервной копии;
* Восстановление случайно изменённых данных без наличия резервной копии;
* Восстановление данных после случайного удаления или изменения;
* Быстрый поиск объектов и данных в БД;
* Восстановление удалённых данных из журналов транзакций.

Особенности доступных инструментов на рынке можно сопоставить в сравнительной таблице.

Таблица 1.4.

Характеристики систем автоматизации синхронизации данных.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № | Название | Возможность синхронизации с базой данных | Возможность синхронизации файлов | Защищённое соединение | Стоимость, руб. |
| п/п |  |  |
|  |  |
| 1. | BatchSync Secure | нет | да | да | От 34742 |
| 2. | SymmetricDS | нет | да | нет | бесплатно |
| 3. | ApexSQL  Data Diff | да | нет | нет | От 23200 |

Целью дипломной работы является создание системы автоматизации управления видеонаблюдением в аудиториях проведения экзаменов ГИА ЕГЭ(ОГЭ). Необходимость создания автоматизированной системы вызвана несколькими основными соображениями. Во-первых, это регулярность выгрузки данных. Во-вторых, это точность и своевременность обновления информации об аудиториях, участвующих в видеонаблюдении. В-третьих, это разгрузка специалистов от рутинной и однообразной работы, которую вполне возможно переложить на компьютер.

Поддержание системы в бумажном виде или в виде электронных писем становится чрезмерно трудоёмким, а зачастую чреватый ошибками, способом. Поэтому и требуется решить данную задачу с помощью автоматизации.

Автоматизация позволяет задействовать минимальное количество сотрудников для контроля и выполнения данной задачи.

Используя автоматизированную систему, сотрудник получает возможность не только вовремя отправлять данные, но и имеет возможность гибко управлять расписанием отправки данных, в зависимости от изменений календарного плана занятий на отдельный период сдачи экзаменов, либо на несколько сразу, если заранее известно расписание проведения экзаменов.

При выполнении диплома была сразу взята ориентация на разработку собственной системы, а не на использование какой-либо из существующих. Это было сделано по той причине, что существующие системы рассчитаны на простые схемы, которые трудно применить в условиях специфических систем функционирования и систем безопасности организации.

Таким образом, в данном случае стоит не выбор существующей системы, а разработка системы самостоятельно.

Учитывая достоинства готовых сторонних инструментов и, принимая во внимание стоящую задачу, данный выбор программных средств является оптимальным.

* + 1. Выбор и обоснование стратегии автоматизации задачи

Понятие «стратегии автоматизации» обычно означает выбор того набора бизнес процессов, действий или операций, которые совершаются сотрудниками, клиентами и партнерами или другими участниками внешней среды при взаимодействии с компанией для достижения поставленных целей.

Подходы к автоматизации могут быть различными, в зависимости от выбранного направления можно рассматривать следующие варианты стратегии:

Хаотичная (кусочная) автоматизация.

Это автоматизация одного или нескольких участков работ, а именно задач, решаемых одним или несколькими сотрудниками того отдела или иного отдела без привязки к существующим на предприятии бизнес-процессам. Этот способ характерен для следующих случаев: инвестиционные ресурсы предприятия недостаточны для решения задачи автоматизации в полном объеме; существуют участки, где применение дает значительный экономический эффект, например, за счет сокращения персонала; технология работы или иные условия не позволяют обходиться без применения автоматизированных систем. Чтобы автоматизация по участкам была эффективна, необходима разработка непосредственных планов автоматизации.

Автоматизация по направлениям.

Для повышения эффективности процесса автоматизации по направлениям деятельности также необходимы стратегический и тактический планы автоматизации. Планы должны пересматриваться после окончания автоматизации какого-либо бизнес-процесса и оценки полученных результатов.

Комплексная (полная) автоматизация.

Комплексная автоматизация предполагает распространение на все функции требования к качеству управления процессом внедрения системы. Выбор одной или комбинации из стратегий автоматизации определяется результатом анализа текущего и планируемого состояния предприятия на определенный период. При этом конкретизируется набор функций системы автоматизации, который будет содержать выбранное решение, для удовлетворения потребностей организации.

Автоматизация по участкам предусматривает автоматизацию отдельных производственных участков, объединенных по набору выполняемых функций. Этот способ автоматизации выбирается при условии, если существуют участки, где применение автоматизированных систем дает значительный экономический эффект, например, за счёт сокращения численности персонала.

Автоматизация по направлениям подразумевает под собой автоматизацию отдельных направлений деятельности компании. В этом случае компания получает полную автоматизацию работы, например, кадровой службы, производства, бухгалтерии или логистики. Такой подход к автоматизации вполне нормален и в дальнейшем интеграция уже автоматизированных направлений в рамках всего предприятия не будет связана с серьезными препятствиями.

Хаотичная стратегия не подходит в нашем случае, так как стоит цель автоматизировать фактически работу целого отдела, при этом используется несколько составляющих ИС: сервис, СУБД, клиентское приложение. Нельзя автоматизировать только часть из них, значимого эффекта от этого наблюдаться не будет.

Полная стратегия автоматизации тоже не подходит в данном случае, так как мы автоматизируем одно из направлений деятельности организации.

Стратегия автоматизации по участкам лучше всего подходит в данном дипломном проекте, потому что в нашем случае автоматизируется деятельность одного отдела, отдела работы с регионами, в котором работает 20 человек, которые заняты работой с регионами, но которым приходится остальное время заниматься рутинной работой с получением и компиляцией данных по видеонаблюдению. Автоматизировав данный процесс, можно будет сократить занятость данного отдела, не понижая продуктивность его работы.

Вывод – оптимальным будет использование стратегии автоматизирования по участкам, поскольку данная стратегия наиболее полно отвечает потребностям поставленной задачи.

* + 1. Выбор и обоснование способа приобретения ИС для автоматизации комплекса задач

Для автоматизации процессов управления и информационного обеспечения рассматриваются несколько способов получения готового программного обеспечения:

* Покупка готовой специализированной ИС;
* Покупка системы сторонней организации и её доработка;
* Разработка ИС своими силами;

Покупка готовой специализированной ИС сопряжена со следующими недостатками:

* + Невозможность автоматизировать внутренние сложные бизнес-процессы, для которых нет типовых решений;
  + Трудоёмкость внедрения готовой ИС из-за требований безопасности организации;
  + Отсутствие гибкости готовой системы, из-за невозможности изменения системы;
  + Надёжность системы гарантируется только компанией-разработчиком.

Покупка системы сторонней организации и её доработка сопряжена со следующими недостатками:

* + Сложность автоматизации внутренних бизнес-процессов;
  + Высокая стоимость внедрения;
  + Частичное соответствие потребностям поставленной задачи.

Разработка ИС своими силами имеет следующие недостатки:

* + Трудозатраты собственных сотрудников организации по разработке, тестированию и внедрению системы.

Таким образом, наиболее удобным и выгодным является собственная разработка ИС.

Преимуществом данного решения будет возможность параллельной работы в системе без кардинальных изменений во время доработки, также максимальное количество учтённых пожеланий и строгое соответствие ТЗ при доработке функционала. Данный вариант оптимально подходит также потому, что если что-то пойдет не так, то всегда можно остановится, проанализировать и начать итерацию сначала, вместе с тем, основная система будет продолжать функционировать исправно. Также кроме возможности откатиться и начать сначала, в условиях ограниченности бюджета, данный вариант будет единственным верным решением.

## Обоснование проектных решений

* + 1. Обоснование проектных решений по информационному обеспечению

Информационное обеспечение (ИО) включает в себя:

* систему классификации и кодирования;
* систему унифицированной документации, используемой в ИО;
* информационную базу.

Классификатор - это систематизированных свод наименований группировок объектов, признаков и их кодовых обозначений. Классификаторы служат средством описания данных, обуславливают единство классификации и кодирования информации и предназначены для обеспечения машинной обработки и выдачи данных в удобной форме потребителям при решении различных задач. В зависимости от применения они делятся на три группы:

* общегосударственные классификаторы,
* отраслевые (ведомственные) классификаторы, используемые в пределах определенной отрасли (ведомства);
* локальные классификаторы, используемые в пределах организации или группы организации.

В данном дипломном проекте будет использоваться только локальный классификатор, так как никаких других классификаторов РФ в системе не используется.

Значительную долю внемашинного информационного обеспечения составляет документация. В условиях автоматизации важное значение придается унификации документации, устанавливающей единые требования к содержанию и построению документов. Унифицированные формы документов вырабатываются как для всех предприятий РФ (например, формы бухгалтерской отчетности), так и для отдельных предприятий (например, формы управленческой отчетности). Унификация заключается в тщательном отборе и четком определении необходимой номенклатуры документов. При этом определяются сферы назначения и использования документов и выявляются специфические особенности, характерные для соответствующих видов документов. Документы могут быть унифицированными и локальными.

В данном дипломном проекте использован локальный документ: «Отчёт по видеонаблюдению по регионам». Информационные файлы формируются на основе исходной информации, содержащейся в вышеуказанном первичном документе - основном носителях первичной экономической информации в системах машинной обработки данных. К нему предъявляется ряд требований:

* достаточная полнота информации для решения задачи;
* исключение избыточности информации;
* достоверность и своевременность информации;
* согласованность форм первичных документов с макетами размещения информации на машинном носителе;
* логичность построения документа.

Существует три способа организации информационной базы: файловая организация информационной базы; интегрированная информационная база, смешанная организация информационной базы.

Под файловой организацией информационной базы понимается локальное размещение базы на компьютере, доступ к которому других пользователей осуществляется стандартными методами операционной системы для обмена данными по сети. Под смешанной организацией информационной базы подразумевается распределённая база данных, хранящаяся на нескольких серверах и реплицирующая изменения в каждой из них по расписанию, данная структура информационной базы используется в системах класса ERP для работы в одной информационной базы территориально удалённым офисам одновременно.

Интегрированный способ организации информационной базы представляет собой совокупность взаимосвязанных и хранящихся вместе данных при такой минимальной избыточности, которая допускает их использование оптимальным образом для любых приложений и при этом обеспечивается независимость данных от программы, а для актуализации данных используется общий способ управления.

В данном дипломном проекте наиболее целесообразной организацией информационной базы считаю интегрированную организацию информационной базы, так как размер базы будет увеличиваться каждый день в среднем на 100-300 записей. И оптимальным выбором будет использование СУБД вместо файлового хранения базы данных.

Существует три модели логической структуры базы данных (по способу установления связей между данными): иерархическая, сетевая и реляционная.

В иерархической модели каждой информационной единице (сегменту), кроме корневого, соответствует один исходный сегмент и между исходным и порожденным сегментом устанавливается только одна связь. В иерархических моделях экземпляру исходного сегмента соответствует в общем случае какое-то число экземпляров порожденного сегмента. Такие структуры удобны для отображения отношений типа «один ко многим» в предметной области. Просмотр иерархической структуры возможен только с корневой вершины. Пропуск сегмента в иерархическом пути при доступе к заданному сегменту не допускается. Основные недостатки иерархической структуры: трудность (неэффективность) отображения отношений типа «многие ко многим»; длительность доступа к сегментам, находящимся на нижних уровнях иерархии; ориентированность на определенный тип (разрез) запроса.

Сетевые модели графически отображаются в виде графа. Вершинам графа соответствуют составные единицы информации (записи). Экземпляры записей образуют файлы. Структура записи может быть иерархической или линейной в зависимости от системы. Между парой типов записей может быть объявлено несколько связей, имена и направления связей должны быть четко обозначены. Недостатками являются: сложность (очень большое число параметров описания данных и операторов), а также неудобство навигационного доступа.

Реляционная база данных - это множество отношений. Реляционная модель основана на математической логике и является простейшей и наиболее привычной формой представления данных в виде таблицы. Строка таблицы эквивалентна записи файла базы данных, а колонка - полю записи. Доступ к элементу данных осуществляется посредством связи требуемой строки (записи) с требуемой колонкой (полем). Достоинством реляционной модели является сравнительная простота инструментальных средств ее поддержки, недостатком - жесткость структуры данных (например, невозможность задания строк таблицы произвольной длины) и зависимость скорости ее работы от размера базы данных.

Преимущества использования реляционных базы данных состоит в следующем:

* Простота - в реляционной модели данных существует всего одна информационная конструкция, которая формализует табличное представление данных, привычное для пользователей;
* Теоретическое обоснование - наличие теоретически обоснованных методов нормализации отношений позволяет получать базы данных с заранее заданными свойствами (в основном, с гарантией минимальной избыточности представления данных);
* Независимость данных - когда необходимо изменить структуру реляционной базы данных, то это приводит к минимальным изменениям в программном продукте.

Моделью логической структуры базы данных была выбрана именно реляционная, так как она позволяет довольно быстро сформировать связи между таблицами для правильного построения запросов к базе данных и также легко разорвать эти связи и создать новые для построения другого запроса. Кроме того, архитектура построения связи более проста и время выполнения запроса в реляционной модели выше чем при использовании сетевой или иерархической структуры.

Исходные сведения для решения обозначенной задачи получают из таких источников как базы данных регионального уровня и заявка на поставку данных видеонаблюдения.

Результаты решения задачи отображаются в таких отчетах и документах, как:

- Отчёт по региону;

- Сводный отчёт по регионам;

- Акт поставки данных.

Для решения поставленной задачи задействованы такие классификаторы объектов, как: города, регионы, аудитории, участвующие в видеонаблюдении.

* + 1. Обоснование проектных решений по программному обеспечению

Программное обеспечение (ПО) - совокупность программ системы обработки данных и программных документов, необходимых для эксплуатации этих программ. ПО предназначено для придания вычислительной системе определенных свойств, связанных с увеличением производительности, повышением достоверности получаемых результатов, повышением надежности функционирования системы, улучшения работы пользователя.

Рассмотрим серверное программное обеспечение. Сервера работают под управлением операционной системы Windows Server 2008.

Если рассмотреть доступные для выбора серверные операционные системы, то ими являются:

* 1. Операционная система Red Hat Enterprise Linux. Сертифицированная ФСТЭК операционная система «Red Hat Enterprise Linux Server» является операционной системой со встроенными средствами защиты от несанкционированного доступа к информации, не содержащей сведения, составляющие государственную тайну, и соответствует требованиям руководящих документов «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) — по 5 классу защищенности.
  2. Серверная операционная система Microsoft Windows Server 2008 (все издания), включая сервер виртуализации Hyper-V является сертифицированным ФСТЭК решением.

Для взаимодействия с ПАО «Ростелеком» используется система контроля версий «Git».

Система контроля версий (СКВ) — это система, регистрирующая изменения в одном или нескольких файлах с тем, чтобы в дальнейшем была возможность вернуться к определённым старым версиям этих файлов.

Главное отличие Git'а от любых других СКВ (например, Subversion и ей подобных) — это то, как Git смотрит на свои данные. В принципе, большинство других систем хранит информацию как список изменений (патчей) для файлов. Эти системы (CVS, Subversion, Perforce, Bazaar и другие) относятся к хранимым данным как к набору файлов и изменений, сделанных для каждого из этих файлов во времени.

Git не хранит свои данные в таком виде. Вместо этого Git считает хранимые данные набором слепков небольшой файловой системы. Каждый раз, когда фиксируется текущая версия проекта, Git, по сути, сохраняет слепок того, как выглядят все файлы проекта на текущий момент. Ради эффективности, если файл не менялся, Git не сохраняет файл снова, а делает ссылку на ранее сохранённый файл.

Git больше похож на небольшую файловую систему с невероятно мощными инструментами, работающими поверх неё, чем на просто СКВ.

Для совершения большинства операций в Git'е необходимы только локальные файлы и ресурсы, т.е. обычно информация с других компьютеров в сети не нужна. Это отличает его от централизованных СКВ.

Git следит за целостностью данных. Перед сохранением любого файла Git вычисляет контрольную сумму, и она становится индексом этого файла. Поэтому невозможно изменить содержимое файла или каталога так, чтобы Git не узнал об этом. Эта функциональность встроена в сам фундамент Git'а и является важной составляющей его философии. Если информация потеряется при передаче или повредится на диске, Git всегда это выявит.

Механизм, используемый Git'ом для вычисления контрольных сумм, называется SHA-1 хешем. Это строка из 40 шестнадцатеричных символов (0-9 и a-f), вычисляемая в Git'е на основе содержимого файла или структуры каталога. Фактически, в своей базе данных Git сохраняет всё не по именам файлов, а по хешам их содержимого.

Каталог Git'а — это место, где Git хранит метаданные и базу данных объектов вашего проекта. Это наиболее важная часть Git'а, и именно она копируется, когда клонируется репозиторий с другого компьютера.

Рабочий каталог — это извлечённая из базы копия определённой версии проекта. Эти файлы достаются из сжатой базы данных в каталоге Git'а и помещаются на диск для того, чтобы их можно было просматривать и редактировать.

Область подготовленных файлов — это обычный файл, обычно хранящийся в каталоге Git'а, который содержит информацию о том, что должно войти в следующий коммит. Иногда его называют индексом (index), но в последнее время становится стандартом называть его областью подготовленных файлов (staging area).

Стандартный рабочий процесс с использованием Git'а выглядит примерно так:

1. Вносятся изменения в файлы в своём рабочем каталоге.
2. Подготавливаются файлы, добавляются их слепки в область подготовленных файлов.
3. Делается коммит, который берёт подготовленные файлы из индекса и помещает их в каталог Git'а на постоянное хранение.
4. Отправляются в удалённый репозиторий(необязательно).
   * 1. Обоснование проектных решений по техническому обеспечению

# Проектная часть

## Разработка проекта автоматизации

Модель жизненного цикла - структура, содержащая процессы, действия и задачи, которые осуществляются в ходе разработки, функционирования и сопровождения программного продукта в течение всей жизни системы, от определения требований до завершения ее использования. Существует несколько моделей и стандартов, в той или иной степени регламентирующих жизненный цикл, большинство из них относятся к заказному ПО (автоматизированным системам АС, и др.) и кроме непосредственно ЖЦ регламентируют также и процессы разработки.

ГОСТ 34.601-90 распространяется на автоматизированные системы и устанавливает стадии и этапы их создания. Кроме того, в стандарте содержится описание содержания работ на каждом этапе. Стадии и этапы работы, закрепленные в стандарте, в большей степени соответствуют каскадной модели жизненного цикла.

ISO/IEC 12207:1995 стандарт на процессы и организацию жизненного цикла. Распространяется на все виды заказного ПО. Стандарт не содержит описания фаз, стадий этапов.

Rational Unified Process (RUP) предлагает итеративную модель разработки, включающую четыре фазы: начало, исследование, построение и внедрение. Каждая фаза может быть разбита на этапы (итерации), в результате которых выпускается версия для внутреннего или внешнего использования. Прохождение через четыре основные фазы называется циклом разработки, каждый цикл завершается генерацией версии системы. Если после этого работа над проектом не прекращается, то полученный продукт продолжает развиваться и снова минует те же фазы. Суть работы в рамках RUP - это создание и сопровождение моделей, а не бумажных документов, поэтому этот процесс привязан к использованию конкретных средств моделирования (UML), а также конкретной технологии проектирования и разработки (объектно-ориентированный анализ, объектно-ориентированное программирование).

Custom Development Method (и методика Oracle) по разработке прикладных информационных систем под заказ - конкретный материал, детализированный до уровня заготовок проектных документов, рассчитанных на использование в проектах с применением Oracle. Степень адаптивности CDM ограничивается тремя моделями ЖЦ: "классическая" (предусмотрены все работы/задачи и этапы), "быстрая разработка" (Fast Track), "облегченный подход", рекомендуемый в случае малых проектов и возможности быстро прототипировать приложения.

Microsoft Solution Framework (MSF) сходна с RUP, так же включает четыре фазы: анализ, проектирование, разработка, стабилизация, является итерационной, предполагает использование объектно-ориентированного моделирования. MSF в сравнении с RUP в большей степени ориентирована на разработку бизнес-приложений.

Extreme Programming (XP). Экстремальное программирование является самым новым среди рассматриваемых методологий, сформировалось в 1996 году. В основе методологии командная работа, эффективная коммуникация между заказчиком и исполнителем в течение всего проекта по разработке ИС, а разработка ведется с использованием последовательно дорабатываемых прототипов.

Для разрабатываемых программных модулей больше подходит стандарт ISO/IEC 12207 и ГОСТ 34.601-90. Эти стандарты имеют набор процессов, действий и задач, охватывающий наиболее широкий спектр возможных ситуаций при максимальной адаптируемости.

* + 1. Этапы жизненного цикла проекта автоматизации
    2. Ожидаемые риски на этапах жизненного цикла и их описание

Процесс разработки программного обеспечения связан с определенными рисками, возникающими на всех этапах работ - от этапа Управления требованиями и до внедрения готового продукта.

Процесс управления рисками представляет собой процесс выявления, контроля и устранения или минимизации последствий непредсказуемых событий.

Практически все риски вне зависимости от категорий, источников, подходов к управлению ими можно классифицировать с нескольких различных позиций:

Собственный и предельный риски.

Классификация оценок рисков операции, финансового инструмента вне и внутри некоторой деятельности, портфеля.

Собственный риск - оценка риска отдельной операции, финансового инструмента отдельно от контекста проведения операции или портфеля, в который входит финансовый инструмент.

Предельный риск - величина, на которую изменится оценка риска деятельности, портфеля в целом при добавлении в них оцениваемой операции или финансового инструмента. При осуществлении процедур управления рисками именно предельный риск представляет наибольший интерес, однако получение его технически более сложно, чем получение собственного риска.

Статический и динамический риски.

Классификация рисков с точки зрения их значимости для организации.

Динамический риск - это риск случайных колебаний результатов деятельности, как в лучшую, так и в худшую строну не способные значимо повлиять на жизнеспособность организации. Как правило, это спекулятивные риски, которые при принятии их организацией слабо коррелируют друг с другом.

Статический риск - риск возникновения событий, ситуаций, в результате возникновения которых под угрозу ставится дальнейшая деятельность организации, жизнеспособность отдельных направлений деятельности, отдельных проектов. Это риск качественных, катастрофических потерь в результате поднесения, которых организация уже не сможет функционировать в прежнем режиме.

Систематический и несистематический риски.

Классификация рисков с точки их отображения в модели рисков.

Систематический риск - это риск, связанный с факторами, рассматриваемыми как значимые в рамках некоторой модели. Систематические риски не должны значимо снижаться в рамках большого портфеля или с течением времени, в противном случае факторы, их определяющие целесообразно игнорировать и данные риски могут быть отнесены к несистематическим. Систематические риски являются основным предметом исследования при оценке и управлении рисками.

Несистематический риск - риск, источники которого и чувствительность к которому не рассматриваются в рамках модели оценки и управления рисками. При построении адекватной модели несистематические риски не должны приводить к сколько-либо значимым потерям, и при большом их числе не должны быть связаны друг с другом. В отношении несистематических рисков должен действовать закон больших чисел - выявленные при анализе отдельных элементов деятельности организации, отдельных составляющих некоторого портфеля ценных бумаг, на каком-то небольшом промежутке времени в совокупности в целом по организации, портфелю или с течением времени их вклад в возможные потери будет стремиться к нулю. Несистематические риски, как правило, игнорируются при решении задач оценки и управления рисками.

* + 1. Организационно-правовые и программно-аппаратные средства обеспечения информационной безопасности и защиты информации

Конфиденциальную информацию можно разделить на предметную и служебную. Служебная информация (например, пароли пользователей) не относится к определенной предметной области, в информационной системе она играет техническую роль, но ее раскрытие особенно опасно, поскольку оно чревато получением несанкционированного доступа ко всей информации, в том числе предметной.

Даже если информация хранится в компьютере или предназначена для компьютерного использования, угрозы ее конфиденциальности могут носить некомпьютерный и вообще нетехнический характер.

Многим людям приходится выступать в качестве пользователей не одной, а целого ряда систем (информационных сервисов). Если для доступа к таким системам используются многоразовые пароли или иная конфиденциальная информация, то наверняка эти данные будут храниться не только в голове, но и в записной книжке или на листках бумаги, которые пользователь часто оставляет на рабочем столе или теряет. И дело здесь не в неорганизованности людей, а в изначальной непригодности парольной схемы. Невозможно помнить много разных паролей; рекомендации по их регулярной (по возможности - частой) смене только усугубляют положение, заставляя применять несложные схемы чередования или вообще стараться свести дело к двум-трем легко запоминаемым (и столь же легко угадываемым) паролям.

Описанный класс уязвимых мест можно назвать размещением конфиденциальных данных в среде, где им не обеспечена (и часто не может быть обеспечена) необходимая защита. Помимо паролей, хранящихся в записных книжках пользователей, в этот класс попадает передача конфиденциальных данных в открытом виде (в разговоре, в письме, по сети), которая делает возможным их перехват. Для атаки могут использоваться разные технические средства (подслушивание или прослушивание разговоров, пассивное прослушивание сети и т. п.), но идея одна - осуществить доступ к данным в тот момент, когда они наименее защищены.

Угрозу перехвата данных следует принимать во внимание не только при начальном конфигурировании ИС, но и, что очень важно, при всех изменениях. Весьма опасной угрозой являются выставки, на которые многие организации отправляют оборудование из производственной сети со всеми хранящимися на них данными. Остаются прежними пароли, при удаленном доступе они продолжают передаваться в открытом виде.

Еще один пример изменения: хранение данных на резервных носителях. Для защиты данных на основных носителях применяются развитые системы управления доступом; копии же нередко просто лежат в шкафах, и получить доступ к ним могут многие.

Перехват данных - серьезная угроза, и если конфиденциальность действительно является критичной, а данные передаются по многим каналам, их защита может оказаться весьма сложной и дорогостоящей. Технические средства перехвата хорошо проработаны, доступны, просты в эксплуатации, а установить их, например, на кабельную сеть, может кто угодно, так что эта угроза существует не только для внешних, но и для внутренних коммуникаций.

Кражи оборудования являются угрозой не только для резервных носителей, но и для компьютеров, особенно портативных. Часто ноутбуки оставляют без присмотра на работе или в автомобиле, иногда просто теряют.

Опасной нетехнической угрозой конфиденциальности являются методы морально-психологического воздействия, такие как маскарад - выполнение действий под видом лица, обладающего полномочиями для доступа к данным.

К неприятным угрозам, от которых трудно защищаться, можно отнести злоупотребление полномочиями. На многих типах систем привилегированный пользователь (например, системный администратор) способен прочитать любой (незашифрованный) файл, получить доступ к почте любого пользователя и т. д. Другой пример - нанесение ущерба при сервисном обслуживании. Обычно сервисный инженер получает неограниченный доступ к оборудованию и имеет возможность действовать в обход программных защитных механизмов.

Методы защиты

Существующие методы и средства защиты информации компьютерных систем (КС) можно подразделить на четыре основные группы:

методы и средства организационно-правовой защиты информации;

методы и средства инженерно-технической защиты информации;

криптографические методы и средства защиты информации;

программно-аппаратные методы и средства защиты информации.

Методы и средства организационно-правовой защиты информации

К методам и средствам организационной защиты информации относятся организационно-технические и организационно-правовые мероприятия, проводимые в процессе создания и эксплуатации КС для обеспечения защиты информации. Эти мероприятия должны проводиться при строительстве или ремонте помещений, в которых будет размещаться КС; проектировании системы, монтаже и наладке ее технических и программных средств; испытаниях и проверке работоспособности КС.

На этом уровне защиты информации рассматриваются международные договоры, подзаконные акты государства, государственные стандарты и локальные нормативные акты конкретной организации.

Методы и средства инженерно-технической защиты

Под инженерно-техническими средствами защиты информации понимают физические объекты, механические, электрические и электронные устройства, элементы конструкции зданий, средства пожаротушения и другие средства, обеспечивающие:

защиту территории и помещений КС от проникновения нарушителей;

защиту аппаратных средств КС и носителей информации от хищения;

предотвращение возможности удаленного (из-за пределов охраняемой территории) видеонаблюдения (подслушивания) за работой персонала и функционированием технических средств КС;

предотвращение возможности перехвата ПЭМИН (побочных электромагнитных излучений и наводок), вызванных работающими техническими средствами КС и линиями передачи данных;

организацию доступа в помещения КС сотрудников;

контроль над режимом работы персонала КС;

контроль над перемещением сотрудников КС в различных производственных зонах;

противопожарную защиту помещений КС;

минимизацию материального ущерба от потерь информации, возникших в результате стихийных бедствий и техногенных аварий.

Важнейшей составной частью инженерно-технических средств защиты информации являются технические средства охраны, которые образуют первый рубеж защиты КС и являются необходимым, но недостаточным условием сохранения конфиденциальности и целостности информации в КС.

Криптографические методы защиты и шифрование

Шифрование является основным средством обеспечения конфиденциальности. Так, в случае обеспечения конфиденциальности данных на локальном компьютере применяют шифрование этих данных, а в случае сетевого взаимодействия - шифрованные каналы передачи данных.

Науку о защите информации с помощью шифрования называют криптографией (криптография в переводе означает загадочное письмо или тайнопись).

Криптография применяется:

* для защиты конфиденциальности информации, передаваемой по открытым каналам связи;
* для аутентификации (подтверждении подлинности) передаваемой информации;
* для защиты конфиденциальной информации при ее хранении на открытых носителях;
* для обеспечения целостности информации (защите информации от внесения несанкционированных изменений) при ее передаче по открытым каналам связи или хранении на открытых носителях;
* для обеспечения неоспоримости передаваемой по сети информации (предотвращения возможного отрицания факта отправки сообщения);
* для защиты программного обеспечения и других информационных ресурсов от несанкционированного использования, и копирования.

Программные и программно-аппаратные методы и средства обеспечения информационной безопасности

К аппаратным средствам защиты информации относятся электронные и электронно-механические устройства, включаемые в состав технических средств КС и выполняющие (самостоятельно или в едином комплексе с программными средствами) некоторые функции обеспечения информационной безопасности. Критерием отнесения устройства к аппаратным, а не к инженерно-техническим средствам защиты является обязательное включение в состав технических средств КС.

К основным аппаратным средствам защиты информации относятся:

* устройства для ввода идентифицирующей пользователя информации (магнитных и пластиковых карт, отпечатков пальцев и т. п.);
* устройства для шифрования информации;
* устройства для воспрепятствования несанкционированному включению рабочих станций и серверов (электронные замки и блокираторы).

Примеры вспомогательных аппаратных средств защиты информации:

устройства уничтожения информации на магнитных носителях;

устройства сигнализации о попытках несанкционированных действий пользователей КС и др.

Под программными средствами защиты информации понимают специальные программы, включаемые в состав программного обеспечения КС исключительно для выполнения защитных функций. К основным программным средствам защиты информации относятся:

* программы идентификации и аутентификации пользователей КС;
* программы разграничения доступа пользователей к ресурсам КС;
* программы шифрования информации;
* программы защиты информационных ресурсов (системного и прикладного программного обеспечения, баз данных, компьютерных средств обучения и т. п.) от несанкционированного изменения, использования и копирования.

Под идентификацией, применительно к обеспечению информационной безопасности КС, понимают однозначное распознавание уникального имени субъекта КС. Аутентификация означает подтверждение того, что предъявленное имя соответствует данному субъекту (подтверждение подлинности субъекта).

Примеры вспомогательных программных средств защиты информации:

* программы уничтожения остаточной информации (в блоках оперативной памяти, временных файлах и т. п.);
* программы аудита (ведения регистрационных журналов) событий, связанных с безопасностью КС, для обеспечения возможности восстановления и доказательства факта происшествия этих событий;
* программы имитации работы с нарушителем (отвлечения его на получение якобы конфиденциальной информации);
* программы тестового контроля защищенности КС и др.

## Информационное обеспечение задачи

* + 1. Информационная модель и её описание

На рисунке 1.6. изображена информационная модель ФГБУ «ФЦТ».



Рисунок 1.6. Информационная модель ФГБУ «ФЦТ».

* + 1. Характеристика нормативно-справочной, входной и оперативной информации

База данных состоит из шести таблиц:

1. Справочник административно-территориальных единиц.
2. Справочник аудиторий в ППЭ.
3. Справочник регионов.
4. Справочник ППЭ.
5. Справочник ОИВ субъекта РФ.
6. Справочник школ.

Файл, содержащий расписание работы менеджера задач, является XML файлом, который имеет следующую структуру:

- Коллекция задач

- Задача

- Тэг наименования

- Дата начала

- Дата окончания

- Время срабатывания триггера

- Настройки триггера

- Разовый запуск

- Дата

- Активно

- Ежедневный запуск

- Интервал дней

- Еженедельно

- День недели

- Ежемесячно

- Дни месяца

- По будням

- Будний день

* + 1. Характеристика результатной информации

Файл выгрузки информации по аудиториям, участвующим в видеонаблюдении является XML файлом.

Он имеет следующую структуру:

- Расписание

- Регионы

- Регион

- Список ППЭ

- ППЭ

- Аудитории

- Аудитория

- Предметы

- Предмет

## Программное обеспечение задачи

* + 1. Общие положения (дерево функций и сценарий диалога)

ИС состоит из двух модулей, структурная схема работы которых представлена на Рис 1.7, Рис 1.8 и Рис 1.9.

Модуль, выгружающий данные по расписанию в защищённом контуре сети, работает с заданным интервалом. Его основная задача – регулярная выгрузка данных из БД. Непосредственного интерфейса пользователя данный модуль не имеет. Модуль оформлен как сервис операционной системы Windows, и может иметь возможности сервиса по установке в системе, деинсталляции из системы, запуска, остановки и перезапуска.

Получение выгрузки из базы данных в виде XML

Получение доступа в разделяемый каталог домена внешнего сервера и запись в файл

Рисунок 1.7. Схема работы модуля выгрузки сериализованных данных из защищённого контура.

Модуль, работающий на сервере открытой сети, имеет интерфейс пользователя и сам сервис операционной системы Windows, работающий по заданным настройкам. Основная задача модуля открытой сети – иметь настройки для работы по расписанию для регулярной отправки сериализованных данных конечному потребителю(клиенту).

Пользователь имеет возможность режимы работы в различном виде.

Есть возможность задать как календарные даты и время однократного выполнения, так и регулярную работу ежедневно, с заданным интервалом дней, еженедельно, с указанием конкретных дней недели, ежемесячно, с указанием конкретных дней месяца.

Кроме того, имеется возможность установить режим работы по выбранным будним(рабочим) дням.

Пользователь имеет возможность сохранить или прочитать файл настроек, который сохраняется в системе.

Схема работы пользовательского интерфейса управления модуля открытой сети представлена на Рис 1.8.

Схема работы сервиса открытой сети представлен на Рис 1.9.

Управление работой модуля пользователем

Сохранение или чтение сериализованных параметров работы модуля

Управление сервисом:

1.Установка

2.Деинсталляция

3.Запуск

4.Остановка

Ввод параметров работы

Рисунок 1.8. Схема работы пользовательского интерфейса управления модуля открытой сети.

Чтение параметров работы

Запуск фонового процесса работы по параметрам работы

По событию задачи, фиксация файла выгрузки и отправка в удалённый репозиторий

Рисунок 1.9. Схема работы сервиса открытой сети.

Основной экран интерфейса управления отображён на Рис 1.10.

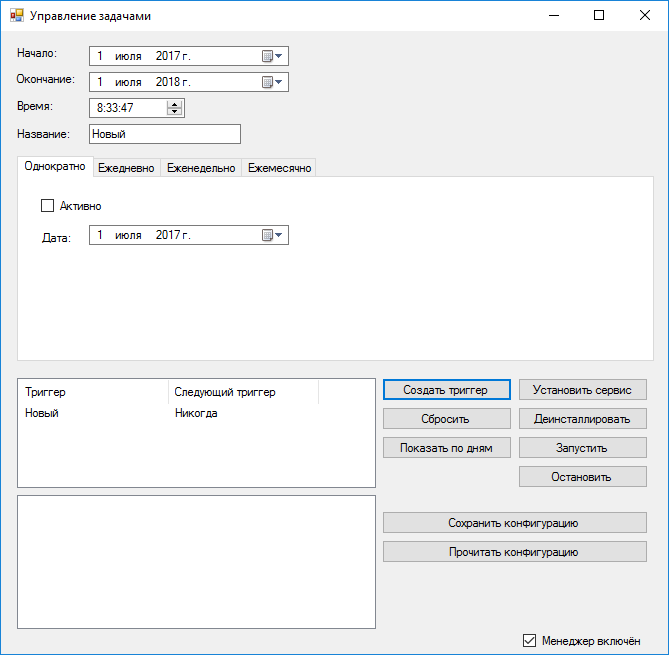


Рисунок 1.10. Основной экран интерфейса управления.

На рисунке 1.11 изображён блок выбора календарного режима работы.

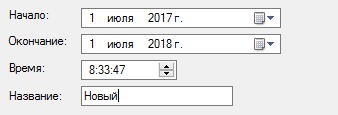


Рисунок 1.11. Блок выбора календарного режима работы.

На рисунке 1.12 изображена вкладка выбора режима ежедневной работы.

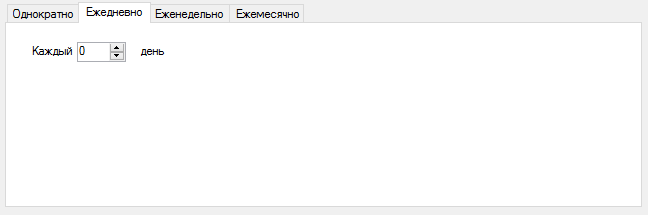


Рисунок 1.12. Вкладка выбора режима ежедневной работы.

На рисунке 1.13 изображена вкладка выбора режима еженедельной работы.

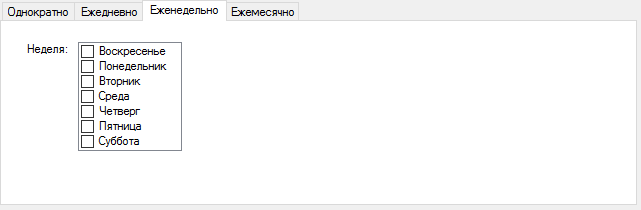


Рисунок 1.13. Вкладка выбора режима еженедельной работы.

На рисунке 1.14 изображена вкладка выбора режима ежемесячной работы.

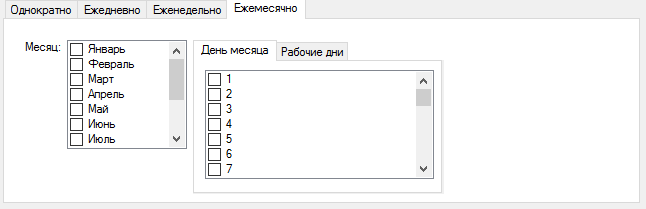


Рисунок 1.14. Вкладка выбора режима ежемесячной работы.

На рисунке 1.15 изображен блок отображения созданных задач(триггеров).

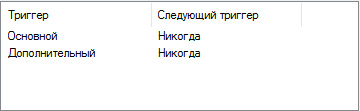


Рисунок 1.15. Блок отображения созданных задач(триггеров).

На рисунке 1.16 изображен блок управления работой сервиса и настроек параметров задач.

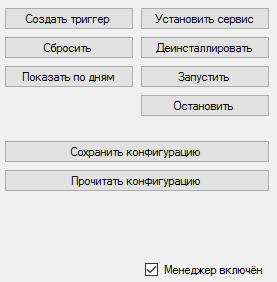


Рисунок 1.16. Блок управления работой сервиса и настроек параметров задач.

* + 1. Характеристика базы данных

База данных системы реализуется на MS SQL Server. Разработаем ER-модель (Entity-Relationship model, модель «сущность-связь») базы данных. ER модель (рисунок 2.7) отображает состав и взаимосвязи таблиц, отражающих содержание информационной модели в терминах конкретной СУБД.

Таблица 1.5.

Перечень сущностей и их соответствие информационной модели

|  |  |  |
| --- | --- | --- |
| № | Название сущности в информационной модели | Идентификатор таблицы |
| 1 | Справочник административно-территориальных единиц | rbd\_Areas |
| 2 | Справочник аудиторий в ППЭ | rbd\_Auditoriums |
| 3 | Справочник регионов | rbdc\_Regions |
| 4 | Справочник ППЭ | rbd\_Stations |
| 5 | Справочник ОИВ субъекта РФ | rbd\_Governments |
| 6 | Справочник школ | rbd\_Schools |

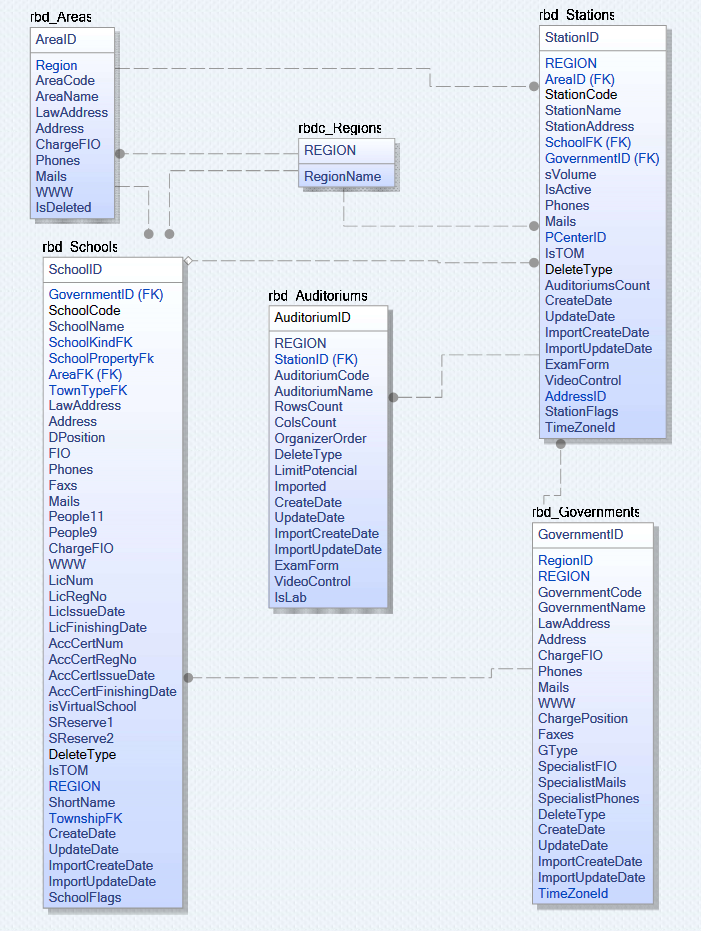


Рисунок 1.8. Структура базы данных.

Структура справочников приведена в таблицах.

Таблица 1.6.

Справочник административно-территориальных единиц rbd\_Areas.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Наименование поля таблицы** | **Тип и размерность поля таблицы** | **Описание поля таблицы** | **Обязательность заполнения поля таблицы** | **Ссылка (таблица)** |
| AreaID | uniqueidentifier(16) | Уникальный идентификатор записи | Да |  |
| Region | int(4) | Код субъекта РФ | Да | rbdс\_Regions |
| AreaCode | int(4) | Код АТЕ | Да |  |
| AreaName | varchar(255) | Название АТЕ | Да |  |
| LawAddress | varchar(255) | Юридический адрес МОУО |  |  |
| Address | varchar(255) | Фактический адрес МОУО |  |  |
| ChargeFIO | varchar(150) | ФИО сотрудника, ответственного за проведение ЕГЭ |  |  |
| Phones | varchar(80) | Телефон(ы) МОУО |  |  |
| Mails | varchar(255) | Адрес(а) электронной почты МОУО |  |  |
| WWW | varchar(255) | WWW – сайт органа МОУО |  |  |
| IsDeleted | bit(1) | Флаг удаленной записи (0 – активная, 1 – удаленная) | Да |  |

Таблица 1.7.

Справочник аудиторий в ППЭ rbd\_Auditoriums.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Наименование поля таблицы** | **Тип и размерность поля таблицы** | **Описание поля таблицы** | **Обязательность заполнения поля таблицы** | **Ссылка (таблица)** |
| REGION | int(4) | Код субъекта РФ | Да | rbdс\_Regions |
| AuditoriumID | uniqueidentifier(16) | Уникальный идентификатор записи | Да |  |
| StationID | uniqueidentifier(16) | Ссылка на ППЭ | Да | rbd\_Stations |
| AuditoriumCode | varchar(4) | Код аудитории | Да |  |
| AuditoriumName | varchar(255) | Наименование аудитории | Да |  |
| RowsCount | int(4) | Количество рядов в аудитории | Да |  |
| ColsCount | int(4) | Количество посадочных мест в ряду | Да |  |
| OrganizerOrder | int(4) | Расположение парт в аудитории (0 – вертикально: 1 - горизонтально) | Да |  |
| DeleteType | int(4) | Признак удаленной строки (0 – активна, не равно 0 – удалена) | Да |  |
| LimitPotencial | int(4) | Признак аудитории для специализированной рассадки | Да |  |
| Imported | bit(1) | Признак импорта |  |  |
| CreateDate | datetime(8) | Дата-время создания | Да |  |
| UpdateDate | datetime(8) | Дата-время последнего изменения | Да |  |
| ImportCreateDate | datetime(8) | Дата-время создания записи |  |  |
| ImportUpdateDate | datetime(8) | Дата-время последнего изменения записи |  |  |
| ExamForm | int(4) | Признак пригодности аудитории для экзаменов в устной/компьютерной форме | Да |  |
| VideoControl | bit(1) | Признак наличия видеонаблюдения в аудитории (0/false – нет, 1/true – есть) | Да |  |
| IsLab | bit(1) | Признак использования аудитории в качестве лаборатории (0/false – не пригодна, 1/true – пригодна) | Да |  |

Таблица 1.8.

Справочник ОИВ rbd\_Governments.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Наименование поля таблицы** | **Тип и размерность поля таблицы** | **Описание поля таблицы** | **Обязательность заполнения поля таблицы** | **Ссылка (таблица)** |
| GovernmentID | uniqueidentifier(16) | Уникальный идентификатор записи | Да |  |
| RegionID | uniqueidentifier(16) | Уникальный идентификатор субъекта РФ | Да | rbd\_CurrentRegion |
| REGION | int(4) | Код субъекта РФ | Да | rbdс\_Regions |
| GovernmentCode | int(4) | Код ОИВ | Да |  |
| GovernmentName | varchar(255) | Полное наименование ОИВ | Да |  |
| LawAddress | varchar(255) | Юридический адрес ОИВ, включая почтовый индекс | Да |  |
| Address | varchar(255) | Фактический адрес ОИВ, включая почтовый индекс |  |  |
| ChargeFIO | varchar(150) | ФИО руководителя ОИВ | Да |  |
| Phones | varchar(80) | Телефон ОИВ | Да |  |
| Mails | varchar(80) | E-mail ОИВ | Да |  |
| WWW | varchar(255) | Адрес WWW – сайта ОИВ |  |  |
| ChargePosition | varchar(150) | Должность руководителя ОИВ | Да |  |
| Faxes | varchar(80) | Факс(ы) ОИВ | Да |  |
| GType | int(4) | Тип ОИВ: 0 Муниципальный ОИВ, 1 ОИВ субъекта РФ, 2 Неизвестный тип | Да |  |
| SpecialistFIO | varchar(150) | ФИО специалиста ОИВ, ответственного за подготовку и проведение ЕГЭ | Да |  |
| SpecialistMails | varchar(80) | E-mail специалиста ОИВ, ответственного за подготовку и проведение ЕГЭ |  |  |
| SpecialistPhones | varchar(255) | Телефон(ы) специалиста ОИВ, ответственного за подготовку и проведение ЕГЭ | Да |  |
| DeleteType | int(4) | Признак удаленной строки (0 – активна, не равно 0 – удалена) | Да |  |
| CreateDate | datetime(8) | Дата-время создания | Да |  |
| UpdateDate | datetime(8) | Дата-время последнего изменения | Да |  |
| ImportCreateDate | datetime(8) | Дата-время создания записи при импорте |  |  |
| ImportUpdateDate | datetime(8) | Дата-время последнего изменения записи при импорте |  |  |
| TimeZoneId | int(4) | Уникальный идентификатор часового пояса |  | rbdc\_RegionTimeZone |

Таблица 1.9.

Справочник школ rbd\_Schools.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Наименование поля таблицы** | **Тип и размерность поля таблицы** | **Описание поля таблицы** | **Обязательность заполнения поля таблицы** | **Ссылка (таблица)** |
| SchoolID | uniqueidentifier(16) | Уникальный идентификатор записи | Да |  |
| GovernmentID | uniqueidentifier(16) | ОИВ, которому непосредственно подчинена ОО | Да | rbd\_ Governments |
| SchoolCode | int(4) | Код ОО | Да |  |
| SchoolName | varchar(1024) | Полное наименование ОО |  |  |
| SchoolKindFK | smallint(2) | Вид ОО | Да | rbdc\_SchoolKinds |
| SchoolPropertyFk | smallint(2) | Организационно-правовая форма ОО | Да | rbdc\_SchoolProperties |
| AreaFK | uniqueidentifier(16) | АТЕ, на территории которой находится ОО | Да | rbd\_Areas |
| TownTypeFK | int(4) | Тип населенного пункта, где расположена ОО | Да | rbdc\_TownTypes |
| LawAddress | varchar(-1) | Юридический адрес ОО, включая почтовый индекс | Да |  |
| Address | varchar(-1) | Фактический адрес ОО, включая почтовый индекс |  |  |
| DPosition | varchar(150) | Должность руководителя ОО | Да |  |
| FIO | varchar(150) | ФИО руководителя ОО | Да |  |
| Phones | varchar(80) | Телефоны ОО | Да |  |
| Faxs | varchar(80) | Факсы ОО |  |  |
| Mails | varchar(255) | E-mail ОО | Да |  |
| People11 | int(4) | Количество обучающихся в выпускных классах | Да |  |
| People9 | int(4) | Количество обучающихся в предвыпускных классах | Да |  |
| ChargeFIO | varchar(150) | ФИО работника, отвечающего за подготовку и проведение ЕГЭ | Да |  |
| WWW | varchar(255) | Адрес WWW – сайта ОО |  |  |
| LicNum | varchar(80) | Номер лицензии на осуществление образовательной деятельности |  |  |
| LicRegNo | varchar(80) | Регистрационный номер лицензии на осуществление образовательной деятельности |  |  |
| LicIssueDate | varchar(10) | Дата выдачи лицензии на осуществление образовательной деятельности |  |  |
| LicFinishingDate | varchar(10) | Дата окончания лицензии на осуществление образовательной деятельности |  |  |
| AccCertNum | varchar(255) | Номер свидетельства о государственной аккредитации |  |  |
| AccCertRegNo | varchar(255) | Регистрационный номер свидетельства о государственной аккредитации |  |  |
| AccCertIssueDate | varchar(10) | Дата выдачи свидетельства о государственной аккредитации |  |  |
| AccCertFinishingDate | varchar(10) | Дата окончания действия свидетельства о государственной аккредитации |  |  |
| isVirtualSchool | bit(1) | Признак «виртуальности ОО» (не используется) |  |  |
| SReserve1 | varchar(255) | Резервное поле |  |  |
| SReserve2 | varchar(255) | Резервное поле |  |  |
| DeleteType | int(4) | Признак удаленной строки (0 – активна, не равно 0 – удалена) | Да |  |
| IsTOM | bit(1) | Флаг расположении ОО в ТОМ (0/false – обычное ОО, 1/true – ОО в ТОМ) | Да |  |
| REGION | int(4) | Код субъекта РФ | Да | rbdс\_Regions |
| ShortName | varchar(255) | Краткое название ОО |  |  |
| TownshipFK | int(4) | Тип территории по ОКАТО | Да | rbd\_Townships |
| CreateDate | datetime(8) | Дата-время создания | Да |  |
| UpdateDate | datetime(8) | Дата-время последнего изменения | Да |  |
| ImportCreateDate | datetime(8) | Дата-время создания записи |  |  |
| ImportUpdateDate | datetime(8) | Дата-время последнего изменения записи |  |  |
| SchoolFlags | int(4) | Дополнительный признак ОО: по умолчанию всегда 0 | Да |  |

Таблица 1.10.

Справочник ППЭ rbd\_Stations.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Наименование поля таблицы** | **Тип и размерность поля таблицы** | **Описание поля таблицы** | **Обязательность заполнения поля таблицы** | **Ссылка (таблица)** |
| StationID | uniqueidentifier(16) | Уникальный идентификатор записи | Да |  |
| REGION | int(4) | Код субъекта РФ | Да | rbdс\_Regions |
| AreaID | uniqueidentifier(16) | АТЕ, на территории которого расположен ППЭ | Да | rbd\_Areas |
| StationCode | int(4) | Код ППЭ | Да |  |
| StationName | varchar(255) | Полное наименование ППЭ | Да |  |
| StationAddress | varchar(1000) | Фактический адрес ППЭ |  |  |
| SchoolFK | uniqueidentifier(16) | ОО, на территории которого расположен ППЭ (если есть) |  | rbd\_Schools |
| GovernmentID | uniqueidentifier(16) | ОИВ, которому подчинен ППЭ | Да | rbd\_Governments |
| sVolume | int(4) | Оценочная вместимость | Да |  |
| IsActive | bit(1) | Не используется |  |  |
| Phones | varchar(255) | Телефон(ы) ППЭ |  |  |
| Mails | varchar(255) | Адрес(а) электронной почты ППЭ | Да |  |
| PCenterID | uniqueidentifier(16) | Не заполняется |  |  |
| IsTOM | bit(1) | Флаг расположении ППЭ в ТОМ (0/false – обычное ОО, 1/true – ОО в ТОМ) | Да |  |
| DeleteType | int(4) | Признак удаленной строки (0 – активна, не равно 0 – удалена) | Да |  |
| AuditoriumsCount | int(4) | Оценочное количество аудиторий |  |  |
| CreateDate | datetime(8) | Дата-время создания | Да |  |
| UpdateDate | datetime(8) | Дата-время последнего изменения | Да |  |
| ImportCreateDate | datetime(8) | Дата-время создания записи |  |  |
| ImportUpdateDate | datetime(8) | Дата-время последнего изменения записи |  |  |
| ExamForm | int(4) | Форма проведения ГИА (4- ЕГЭ, 8- ГВЭ, 12- ЕГЭ, ГВЭ) | Да |  |
| VideoControl | bit(1) | Наличие видеонаблюдения в ППЭ (0/false – нет, 1/true – есть) | Да |  |
| AddressID | uniqueidentifier(16) | Ссылка на таблицу адресов |  | rbd\_Adress |
| StationFlags | int(4) | Дополнительные признаки ППЭ: (1– ППЭ на дому, 2- независимый центр, 4– ЕГЭ, 8- ГВЭ, 16- национальные экзамены, 64 - Отдаленный ППЭ 128 - Резервный ППЭ 512 - ППЭ в учреждении УФСИН 1024 - ППЭ в больнице). если выбрано несколько признаков, то значения складываются. Например, у ППЭ стоят признаки: - ГВЭ (8),  - ППЭ на дому (1),  - Отдаленный ППЭ (64)  => StationFlags=73 | Да |  |
| TimeZoneId | int(4) | Уникальный идентификатор часового пояса |  | rbdc\_TimeZones |

* + 1. Структурная схема пакета (дерево вызова программных модулей)
    2. Описание программных модулей

## Контрольный пример реализации проекта и его описание