ВВЕДЕНИЕ

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

Скорость выполнения задачи зачастую является очень важным преимуществом. Нередко требуется чтобы задача выполнялась с минимальным временем, что в случае с ручной обработкой часто либо невозможно, либо сопряжено с определёнными трудностями.

Человек в любом случае не может конкурировать с компьютером по количеству производимых операций на единицу времени.

Большая часть задач требует максимальной точности выполнения, которой трудно ожидать от человека в постоянном режиме.

Ошибки, возникающие при ручной обработке, зачастую приводят к лавинообразным накоплениям неверных сведений, которые могут приводить к весьма неэффективным результатам работы системы или предприятия в целом.

Высвобождение ресурсов рабочего времени сотрудников позволяет, в первую очередь, задействовать данное время на решение других задач, тем самым подняв производительность. Не в последнюю очередь это позволяет улучшить контроль над процессами автоматизации в том числе.

Важным плюсом является регулярность выполнения. Компьютер, в отличие от человека, не может «забыть» выполнить возложенную на него задачу.

Если от своевременности выполнения зависят какие-то критичные процессы, то это является весомым аргументом в пользу компьютерной автоматизации.

Рутинные операции, неизбежные при массовой обработке, вводу или передачи данных не способствуют качеству ручного труда. Они наоборот способны снижать качество и скорость производимых операций. Также это может угнетающе воздействовать на психику сотрудников. Желательно избегать возложение трудоёмких и кропотливых операций в виде обязательной рутины, если эти задачи можно автоматизировать.

Задача дипломной работы является исследование и реализация процесса автоматизации видеонаблюдения в аудиториях проведения экзаменов.

Автоматизация видеонаблюдения состоит в регулярной и запланированной передаче данных по аудиториям, участвующим в процессе проведения экзаменов.

В последующих главах будет представлено:

* 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.

Приведённая в дипломной работе система позволяет иметь контроль над производимыми регулярными действиями по выгрузке актуальных данных по аудиториям, участвующим в проведении экзаменационных тестов.

При этом использование данной системы со стороны сотрудников организации сводится к своевременному составлению нового календарного плана выгрузки, либо корректировке существующего.

Основные задачи, которые требуется решить в данной работе:

Создание двух сервисов, работающих в защищённой сети и сети общего назначения (с доступом в глобальную сеть интернет).

Сервис номер 1: «Сервис выгрузки данных».

Работает в защищённой сети, проверяет наличие изменения в графике поставленных задач. Выполняет задачи выгрузки сериализованных данных из базы данных по текущему графику.

Сервис номер 2: «Сервис отправки данных».

Работает в сети общего назначения с выходом в глобальную сеть интернет, отправляет файлы с данными при наличии изменившихся данных.

Данная система позволяет иметь контроль над производимыми регулярными действиями по выгрузке актуальных данных по аудиториям, участвующим в проведении экзаменационных тестов.

При этом использование данной системы со стороны сотрудников организации сводится к своевременному составлению нового календарного плана выгрузки, либо корректировке существующего.

Данные, которые передаёт данный программный комплекс, являются нежелательными для распространения в широком доступе, вследствие чего большая часть архитектурной схемы работы направлена на соблюдение безопасности на всех этапах передачи данных.

Это относится как к работе с базой данных в защищённой сети, передаче данных с авторизацией к домену сети общего доступа, и далее передаче данных по сети интернет с использованием системы контроля версий по защищённому каналу с использованием асимметричного шифрования.

**Глава I. Аналитическая часть.**

* 1. **Технико-экономическая характеристика предметной области и предприятия.**
     1. **Характеристика предприятия и его деятельности.**
        1. Полное название предприятия.

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

* + - 1. 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.

* + - 1. 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».

* + - 1. Направления деятельности.

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.

* + 1. **Организационная структура управления предприятием.**

Непосредственное руководство деятельностью Центра осуществляется его директором на принципах единоначалия.

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.



Рисунок 1. Организационная структура ФГБУ «ФЦТ».

**1.1.3 Программная и техническая архитектура ИС предприятия**



Рисунок 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.



Рисунок 3. Программная архитектура ФГБУ «ФЦТ».

**1.2 Характеристика комплекса задач, задачи и обоснование необходимости автоматизации**

**1.2.1 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) 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.

Рисунок 4. Схема существующего бизнес-процесса управления видеонаблюдением

1.2.2. Определение места проектируемой задачи в комплексе задач и ее описание.

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 пользованию.

1.2.3. Обоснования необходимости использования вычислительной техники для решения задачи

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

1.2.4. 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 ИБ и ЗИ: 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 ограничения 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 идентификационный ПИН код, за который он несет материальную ответственность.

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