Министерство науки и высшего образования Российской Федерации

УНИВЕРСИТЕТСКИЙ КОЛЛЕДЖ
федерального государственного бюджетного образовательного учреждения
высшего образования
«Оренбургский государственный университет»

Отделение информационных технологий

Предметно-цикловая комиссия информационной безопасности систем и сетей

ОТЧЕТ

по учебной практике

по ПМ 01 «Эксплуатация автоматизированных (информационных) систем в защищенном исполнении»

Университетский колледж ОГУ 10.02.05 7022.149 П

Руководитель
_____А.Д. Синицина
(подпись, дата)

Исполнитель
студент группы 20ОИБ-1
_____Д.В. Сайфулина
(подпись, дата)

Оренбург 2022

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

УНИВЕРСИТЕТСКИЙ КОЛЛЕДЖ
федерального государственного бюджетного образовательного учреждения
высшего образования
«Оренбургский государственный университет»

Предметно-цикловая комиссия информационной безопасности систем и сетей

Задание на учебную практику

по профессиональному модулю
«Эксплуатация автоматизированных (информационных) систем в
защищенном исполнении»

Провести анализ защищенности объекта заданной предметной области.

Спроектировать компьютерную сеть, выделив объекты для моделирования данной предметной области. Описать порядок прохождения аттестации для объекта информатизации. Реализовать связи между объектами сетевой модели с использованием сетевого симулятора Cisco Packet Tracer. Разработать защиту информации для сформированной компьютерной сети, провести тестирование работоспособности защищенной сети.

Подготовить отчет по практике.

Дата выдачи заданий *«21» ноября 2022 г.*

Руководитель практики _____ А.Д. Синицина
Исполнитель студент группы 20ОИБ-1 _____ Д.В. Сайфулина
Срок защиты работы «10» *декабря* 2022 г.

Оренбург 2022

Содержание

Введение

Развитие компьютерной техники привело к тому, что все большее распространение стали получать информационные системы, базирующиеся на использовании информационно-вычислительной техники и средств коммуникаций, которые являются основными техническими средствами хранения, обработки и передачи информации. Такие информационные системы называют автоматизированными. Они основаны на использовании специальных средств и методов преобразования информации, т.е. автоматизированных информационных технологий.

В данное время ни одно современное предприятие не может быть достаточно конкурентоспособным, если на нем не проводятся усовершенствования и не реализуются новые идеи по автоматизации. Основной целью автоматизации является повышение качества исполнения процесса. Автоматизированный процесс обладает более стабильными характеристиками, чем процесс, выполняемый в ручном режиме. Во многих случаях автоматизация процессов позволяет повысить производительность, сократить время выполнения процесса, снизить стоимость, увеличить точность и стабильность выполняемых операций.

Задачи автоматизации:

- повысить эффективность работы;
- оптимизировать работу;
- сокращение трудоемкости;
- повышение качества;
- сокращение сроков работы.

Цель учебной практики – провести анализ защищенности объекта заданной предметной области, сформировать практические умения по созданию и настройке компьютерной сети, закрепление полученных знаний и приобретения первоначальных практических навыков.

Задачи практики:

- спроектировать компьютерную сеть, выделив объекты для моделирования данной предметной области;
- описать порядок прохождения аттестации для объекта информатизации;
- реализовать связи между объектами сетевой модели с использованием сетевого симулятора Cisco Packet Tracer;
- разработать защиту информации для сформированной компьютерной сети, провести тестирование работоспособности защищенной сети.

1 Теоретическая часть

1.1 Принципы построения защиты информации в операционных системах

Операционная система (ОС) – комплекс взаимосвязанных программ, предназначенных для управления ресурсами компьютера и организации взаимодействия с пользователем [1].

Функции операционной системы:

- управляет всеми ресурсами системы;
- обеспечивает функционирование и правильную координацию процессов устройства;
- упрощает для пользователя работу с устройством.

Самые популярные операционные системы это:

- windows;
- linux;
- mac os;
- android;
- ios.

Защита информации в АС должна основываться на следующих основных принципах:

- системности;
- комплексности;
- непрерывности защиты;
- разумной достаточности;
- гибкости управления и применения;
- открытости алгоритмов и механизмов защиты;
- простоты применения защитных мер и средств.

Принцип системности – системный подход к защите компьютерных систем предполагает необходимость учета всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности АС.

При создании системы защиты необходимо учитывать все слабые, наиболее уязвимые места системы обработки информации, а также характер, возможные объекты и направления атак на систему со стороны нарушителей (особенно высококвалифицированных злоумышленников), пути проникновения в распределенные системы и НСД к информации. Система защиты должна строиться с учетом не только всех известных каналов проникновения и НСД к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

Принцип комплексности – в распоряжении специалистов по компьютерной

безопасности имеется широкий спектр мер, методов и средств защиты компьютерных систем. Комплексное их использование предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов. Защита должна строиться эшелонировано. Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами. Одной из наиболее укрепленных линий обороны призваны быть средства защиты, реализованные на уровне операционных систем (ОС) в силу того, что ОС – это как раз та часть компьютерной системы, которая управляет использованием всех ее ресурсов. Прикладной уровень защиты, учитывающий особенности предметной области, представляет внутренний рубеж обороны [16].

Принцип непрерывности защиты – защита информации – это не разовое мероприятие и даже не определенная совокупность проведенных мероприятий и установленных средств защиты, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла АС, начиная с самых ранних стадий проектирования, а не только на этапе ее эксплуатации.

Разработка системы защиты должна вестись параллельно с разработкой самой защищаемой системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, позволит создать более эффективные (как по затратам ресурсов, так и по стойкости) защищенные системы.

Большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, ключей шифрования, переопределение полномочий и т.п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, для внедрения специальных программных и аппаратных "закладок" и других средств преодоления системы защиты после восстановления ее функционирования.

Разумная достаточность – создать абсолютно непреодолимую систему защиты принципиально невозможно. При достаточном количестве времени и средств можно преодолеть любую защиту. Поэтому имеет смысл вести речь только о некотором приемлемом уровне безопасности. Высокоэффективная система защиты стоит дорого, использует при работе существенную часть мощности и ресурсов компьютерной системы и может создавать ощутимые дополнительные неудобства пользователям. Важно правильно выбрать тот достаточный уровень защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми (задача анализа риска).

Гибкость системы защиты – часто приходится создавать систему защиты в условиях большой неопределенности. Поэтому принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации,
могут обеспечивать как чрезмерный, так и недостаточный уровень защиты.

Естественно, что для обеспечения возможности варьирования уровнем защищенности, средства защиты должны обладать определенной гибкостью. Особенно важным это свойство является в тех случаях, когда установку средств защиты необходимо осуществлять на работающую систему, не нарушая процесса ее нормального функционирования. Кроме того, внешние условия и требования с течением времени меняются. В таких ситуациях свойство гибкости спасает владельцев АС от необходимости принятия кардинальных мер по полной замене средств защиты на новые [17].

Открытость алгоритмов и механизмов защиты – суть принципа открытости алгоритмов и механизмов защиты состоит в том, что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможности ее преодоления (даже автору). Однако, это вовсе не означает, что информация о конкретной системе защиты должна быть общедоступна.

Принцип простоты применения средств защиты – механизмы защиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе законных пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций (ввод нескольких паролей и имен и т.д.)[2].

1.2 Основы информационных систем как объекта защиты

Информационная система – взаимосвязанная совокупность средств, методов и персонала, используемых для хранения, обработки и выдачи информации в интересах достижения поставленной цели [3].

Правила организации и защиты информации в автоматизированных системах описаны Федеральном законе №149-ФЗ «Об информации, информационных технологиях и о защите информации».

В этом законе описаны все основные пункты:

- описание понятия личных сведений;
- описание требований к защите ИС;
- порядок обработки информации.

Обработка информации в информационных системах — это любая совокупность операций (прием, сбор, накопление, хранение, преобразование, отображение, выдача и т.п.), осуществляемых над информацией (фактами, данными, знаниями) с использованием технических средств информационной системы. Специфичным для информационной системы является понятие структуры, которое раскрывает схему связей (физическая структура) и взаимодействия между элементами (логическая структура).

Физическая структура информационной системы — это схема связей таких физических элементов, как технические средства, аппаратура узлов, собственно узлы и вычислительная техника, устанавливаемая в них. К основным компонентам физической структуры можно отнести узлы, каналы и линии связи.

Логическая структура информационной системы определяет принципы установления связей, алгоритмы организации процессов и управления ими, логику функционирования программных средств. В общем виде она определяет соединение и взаимодействие двух принципиально различных по назначению и функциям составных частей архитектуры информационных систем: множества автономных информационных подсистем (узлов) и множества средств их связи и взаимодействия (физических средств соединений) [5].

1.3 Эксплуатация средств защиты информации в компьютерных сетях

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 будут размещаться компьютеры;
- проектировании системы, монтаже и наладке ее технических и программных средств;
- испытаниях и проверке работоспособности компьютерной системы.

Основой проведения организационных мероприятий является использование и подготовка законодательных и нормативных документов в области информационной безопасности, которые на правовом уровне должны регулировать доступ к информации со стороны потребителей. В российском законодательстве позже, чем в законодательстве других развитых стран, появились необходимые правовые акты (хотя далеко не все).

По функциональному назначению средства инженерно-технической защиты делятся на следующие группы:

- физические средства, включающие различные средства и сооружения, препятствующие физическому проникновению (или доступу) злоумышленников на объекты защиты и к материальным носителям конфиденциальной информации и осуществляющие защиту персонала, материальных средств, финансов и информации от противоправных воздействий;
- аппаратные средства – приборы, устройства, приспособления и другие технические решения, используемые в интересах защиты информации. В практике деятельности предприятия находит широкое применение самая различная аппаратура, начиная с телефонного аппарата до совершенных автоматизированных систем, обеспечивающих производственную деятельность. Основная задача аппаратных средств – обеспечение стойкой защиты информации от разглашения, утечки и несанкционированного доступа через технические средства обеспечения производственной деятельности;
- программные средства, охватывающие специальные программы, программные комплексы и системы защиты информации в информационных системах различного назначения и средствах обработки (сбор, накопление, хранение, обработка и передача) данных;
- криптографические средства – это специальные математические и алгоритмические средства защиты информации, передаваемой по системам и сетям связи, хранимой и обрабатываемой на ЭВМ с использованием разнообразных методов шифрования.

Эти средства применяются для решения следующих задач

- охрана территории предприятия и наблюдение за ней;
- охрана зданий, внутренних помещений и контроль за ними;
- охрана оборудования, продукции, финансов и информации;
- осуществление контролируемого доступа в здания и помещения.

Современная криптография включает в себя четыре крупных раздела:

- симметричные криптосистемы. В симметричных криптосистемах и для шифрования, и для дешифрования используется один и тот же ключ. (Шифрование - преобразовательный процесс: исходный текст, который носит также название открытого текста, заменяется шифрованным текстом, дешифрование - обратный шифрованию процесс. На основе ключа шифрованный текст преобразуется в исходный);
- криптосистемы с открытым ключом. В системах с открытым ключом используются два ключа - открытый и закрытый, которые математически связаны друг с другом. Информация шифруется с помощью открытого ключа, который доступен всем желающим, а расшифровывается с помощью закрытого ключа, известного только получателю сообщения.(Ключ - информация, необходимая для беспрепятственного шифрования и дешифрования текстов.);
- электронная подпись. Системой электронной подписи. называется присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения.
- управление ключами. Это процесс системы обработки информации, содержанием которых является составление и распределение ключей между пользователями.

2 Анализ объекта информатизации

2.1 Описание структуры организации

Организационная структура – это система, которая описывает, как определенные действия направляются для достижения целей организации. Эти действия могут включать правила, роли и обязанности. Организационная структура также определяет, как информация перемещается между уровнями внутри компании [6].

Библиотека – это учреждение, собирающее и осуществляющее хранение произведений печати и письменности для общественного пользования, а также ведущее справочно – библиографическую работу.

Библиотеки систематически занимаются сбором, хранением, пропагандой и выдачей читателям произведений печати, а также информационно-библиографической работой [8,9].

Структура Библиотеки предоставлена на рисунке 1 [10].

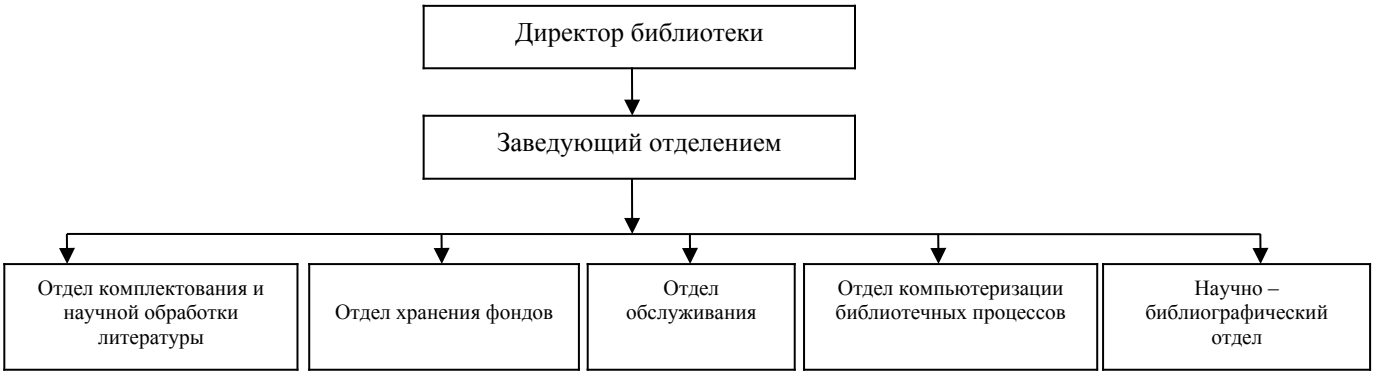


Рисунок 1 – Структура Библиотеки

На рисунке 1 предоставлена структура Библиотеки, на ней видна организационная структура, где Директор контролирует заведующего отделением, а заведующий отделением контролирует следующее отделы:

а) «Отдел комплектования и научной обработки литературы»;

б) «Отдел хранения фондов»;

в) «Отдел обслуживания»;

г) «Отдел компьютеризации библиотечных процессов»;

д) «Научно – библиографический отдел».

В свою очередь « Отдел комплектования и научной обработки литературы» обеспечивает научно обоснованное, полное и оперативное комплектование фонда библиотеки и его учет, разрабатывает и систематически корректирует план комплектования фондов библиотеки в соответствии с образовательно-профессиональными программами, учебными планами и

тематикой научных исследований.

« Отдел хранения фондов» осуществляет формирование, организацию и хранение основной части действующего фонда Библиотеки, состоящей из фонда новых поступлений отечественной литературы и фондов депозитарного хранения отечественной и иностранной литературы.

«Отдел обслуживания» включает в себя: офис главного администратора; административно-хозяйственное подразделение; связь; обслуживающий персонал; службу безопасности.

«Отдел компьютеризации библиотечных процессов» обеспечивает функционирование системы комплексной автоматизации библиотечной деятельности, осваивает новые информационные технологии, адаптирует новое программное обеспечение.

«Научно – библиографический отдел» осуществляет справочно-библиографическое, информационное и консультационное обслуживание пользователей. В фонде отдела находятся справочные издания, энциклопедии и словари по различным отраслям знания. Здесь можно найти путь к поиску необходимой информации, получить консультацию по составлению библиографического списка литературы

2.2 Анализ информационных потоков организации

Информационные потоки – физические перемещения информации от одного сотрудника предприятия к другому или от одного подразделения к другому [9]. Информационные потоки по организации «Библиотека» показаны на рисунке 2.

Виды информационных потоков:

1) по отношению к логистической системе выделяют информационные потоки:

- внутренние – циркулируют в рамках логистической системы или ее отдельного звена;
- внешние – циркулируют между логистической системой и внешней по отношению к логистической системе средой;
- входящие – потоки поступающей в логистическую систему информации из внешней среды;
- выходящие – потоки, исходящие из логистической системы во внешнюю среду.

2) в зависимости от вида систем, связываемых потоком:

- горизонтальный поток – связывает звенья одного уровня иерархии логистической системы;
- вертикальный поток – связывает звенья разных уровней иерархии.

3) по назначению выделяют:

- директивные информационные потоки;
- учетно-аналитические информационные потоки;
- нормативно-справочные информационные потоки;
- вспомогательные информационные потоки.

4) по направлению движения:

- прямой информационный поток – в одном направлении с материальным;
- встречный информационный поток – в обратном направлении к материальному.

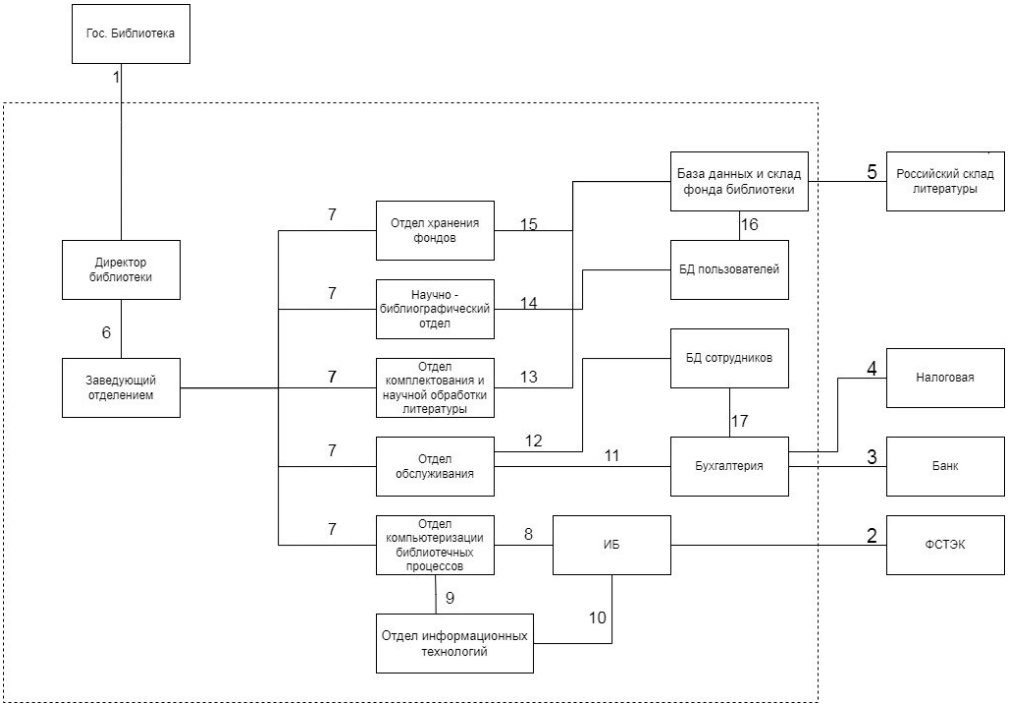


Рисунок 2 – Схема информационных потоков

Таблица 1 – Информационные потоки

Номер информационного потока	Источник документа	Приемник документа	Содержание документа
1 Гос. Библиотека – Директор Библиотеки	Приказы, распоряжения, положения, договора	Директор, Помощник директора	Необходимые регулирующие действия внутри ведомства
2 ФСТЭК – ИБ	Регламентирующие документы, подтверждённые БД угроз	Руководитель отдела ИБ, Работники отдела ИБ	Необходимые регулирующие действия и рекомендации по работе, Действующая БД угроз

Продолжение таблицы 1

3 Банк – Бухгалтерия	Финансовый отчет, Отчет за триместр	Главный бухгалтер, Бухгалтера	Сведение о финансирование каждого отдела, Отчет за триместр
4 Налоговая – Бухгалтерия	Налоговый отчет, Отчет за триместр	Главный бухгалтер, Бухгалтера	Сведенье о налогах каждого отдела, Отчет за триместр
5 Российский склад литературы – База данных и склад фонда библиотеки	Справочно-библиографический аппарат, Система документных коммуникаций	Начальник склада	Регулирующие поставки книг документы, отчетность о получении/отправки
6 Директор библиотеки – Заведующий отделением	Приказы, распоряжения, положения	Заведующий отделением	Необходимые регулирующие действия внутри ведомства
7.1 Заведующий отделением – Отдел хранения фондов	Приказы, распоряжения, положения	Начальник отдела хранения фонда Работники отдела хранения фонда	Необходимые регулирующие действия внутри отдела

Продолжение таблицы 1

7.2 Заведующий отделением – Научно – библиографический отдел	Приказы, распоряжения, положения	Начальник научно – библиографического отдела Работники научно – библиографического отдела	Необходимые регулирующие действия внутри отдела
7.3 Заведующий отделением – Отдел комплектования и научной обработки литературы	Приказы, распоряжения, положения	Начальник отдела комплектования и научной обработки литературы Работники отдела комплектования и научной обработки литературы	Необходимые регулирующие действия внутри отдела
7.4 Заведующий отделением – Отдел обслуживания	Приказы, распоряжения, положения	Начальник отдела обслуживания Работники отдела обслуживания	Необходимые регулирующие действия внутри отдела
7.5 Заведующий отделением – Отдел компьютеризации библиотечных процессов	Приказы, распоряжения, положения	Начальник отдела компьютеризации библиотечных процессов Работники отдела компьютеризации библиотечных процессов	Необходимые регулирующие действия внутри отдела

Продолжение таблицы 1

Номер информационного потока	Источник документа	Приемник документа	Содержание документа
8 Отдел компьютеризации библиотечных процессов – ИБ	Приказы, рекомендации, положения, отчетность за информационную безопасность	Начальник информационной безопасности, Работники ИБ	Приказы и рекомендации в сфере безопасности, Штрафы и наказания за нарушение безопасности, Отчетность по проведениям инструктажа новым работникам
9 Отдел компьютеризации библиотечных процессов – Отдел информационных технологий	Приказы, рекомендации, положения	Начальник информационных технологий Работники ИТ	Необходимые рекомендации и приказы, Отчет проделанной работы в области ИТ
10 ИБ – Отдел информационных технологий	Приказы, рекомендации Приказ в сфере безопасности и информационных технологий	Начальник информационной безопасности, Работники ИТ	Приказ в сфере безопасности и информационных технологий Отчет проделанной работы в области ИТ
11 Отдел обслуживания – Бухгалтерия	Приказы, рекомендации, Финансирование	Главный бухгалтер, Бухгалтера	Необходимые рекомендации и приказы, Отчет финансирование за триместр

Продолжение таблицы 1

Номер информационного потока	Источник документа	Приемник документа	Содержание документа
12 Отдел обслуживания – БД сотрудников	БД сотрудников, Отчет о размерах штаба	Руководитель отдела кадров, Кадровики	ФИО всех сотрудников всех отделов, Информации о работниках всех штабов
13 Отдел комплектования и научной обработки данных – База данных и склад фонда библиотеки	Лист о необходимом завозе, Лист о вывозе	Руководитель склада и его заместитель	Перечень книг на ввоз, Перечень книг на вывоз
14 Научно – библиографический отдел – БД пользователей	Приказы, распоряжения, положения	Начальник отдела по БД пользователей	Необходимые регулирующие действия внутри отдела
15 Отдел хранения фондов – База данных и склад фонда библиотеки	Приказы, распоряжения, положения	Руководитель склада фонда библиотеки Работники склада	Необходимые регулирующие действия внутри отдела

Продолжение таблицы 1

Номер информационного потока	Источник документа	Приемник документа	Содержание документа
16 База данных и склад фонда библиотеки – БД пользователей	Запрос содержания БД, изменения в работе БД, ошибки и неисправности в БД	Начальник отдела по БД пользователей	Содержание БД, информация о работе БД и его ошибках
17 Бухгалтерия – БД сотрудников	Отчет о финансировании, Приказы о выписки заработной платы, Отчет о сотрудниках	Руководитель отдела кадров, Кадровики	Информация о финансировании, ФИО работников и их заработная плата, ФИО уволенных и принятых работниках

В ходе данной части работы, разработав схему информационных потоков, был выявлен принцип построения организации отдела информационной безопасности с другими отделами комитета по противодействию коррупции, а также организации движения информации по всему предприятию.

2.3Анализ АИС предприятия

Информационная система (ИС) — система, предназначенная для хранения, поиска и обработки информации, и соответствующие организационные ресурсы (человеческие, технические, финансовые и т. д.), которые обеспечивают и распространяют информацию (ISO/IEC 2382:2015).

Основное назначение информационной системы – создание современной инфраструктуры для управления предприятием, организацией, учреждением.

Назначение информационной системы состоит в поддержке динамической информационной модели ее предмет ной области.

Задачи:

- обработка данных об операциях, производимых фирмой;
- создание периодических контрольных отчетов о состоянии дел в фирме;
- получение ответов на всевозможные текущие запросы и оформление их в виде бумажных документов или отчетов.

На предприятии должна быть создана база данных, которая обеспечивает хранение информации и доступность её для всех составляющих системы управления. Наличие такой базы данных позволяет сформировать информацию для принятия решений.

Применение базы данных:

- бухгалтерский учет;
- управление финансовыми потоками;
- управление складом, ассортиментом, продуктами, закупками;
- управление производственным процессом;
- управление маркетингом;
- оперативное управление предприятием;
- предоставление информации о фирме.

ИС организационного управления предназначены для автоматизации функций управленческого персонала. Учитывая наиболее широкое применение и разнообразие этого класса систем, часто любые информационные системы понимают именно в данном толковании. К этому классу относятся информационные системы управления, как промышленными фирмами, так и непромышленными объектами: гостиницами, банками, торговыми фирмами и др. Основными функциями подобных систем являются: оперативный контроль и регулирование, оперативный учет и анализ, перспективное и оперативное планирование, бухгалтерский учет, управление сбытом и снабжением и другие экономические и организационные задачи.

ИС управления технологическими процессами (ТП) служат для автоматизации функций производственного персонала по контролю и управлению производственными операциями. В таких системах обычно предусматривается наличие развитых средств измерения параметров технологических процессов (температуры, давления, химического состава и т.п.), процедур контроля допустимости значений параметров и регулирования технологических процессов.

ИС автоматизированного проектирования (САПР) предназначены для автоматизации функций инженеров-проектировщиков, конструкторов, архитекторов, дизайнеров при создании новой техники или технологии. Основными функциями подобных систем являются: инженерные расчеты, создание графической документации (чертежей, схем, планов), создание проектной документации, моделирование проектируемых объектов.

Интегрированные (корпоративные) ИС используются для автоматизации всех функций фирмы и охватывают весь цикл работ от проектирования до сбыта продукции. Они включают в себя ряд модулей (подсистем), работающих в едином информационном пространстве и выполняющих функции поддержки соответствующих направлений деятельности.

В самом широком смысле ИС представляет собой программный комплекс, функции которого состоят в поддержке надежного хранения информации в памяти компьютера, выполнении специфических для данного приложения преобразований информации и/или вычислений, представлении пользователям удобного и легко осваиваемого интерфейса. Технической базой для ИС может быть один отдельный компьютер, локальная или глобальная компьютерная сеть.

С самого начала развития ВТ образовалось два основных направления использования ИС: первое – это применение ВТ для выполнения численных расчетов; второе – использование средств ВТ в автоматизированных информационных системах [7].

На сегодняшний день можно выделить следующие направления применения информационных систем:

- информационно-справочные и информационно-поисковые системы – системы, обеспечивающие поиск и отбор необходимых данных в специальной базе с описаниями источников информации (индексе) на основе информационно-поискового языка и соответствующих правил поиска;
- системы управления взаимоотношениями с клиентами (CRM) – системы, помогающие организации отслеживать, организовывать и анализировать взаимодействие с клиентами по нескольким каналам связи на протяжении всего жизненного цикла клиента;
- системы, обеспечивающие автоматизацию документооборота и учета это автоматизированные многопользовательские системы, сопровождающие процесс управления работой иерархической организации с целью обеспечения выполнения этой организацией своих функций. При этом предполагается, что процесс управления опирается на человеко-читаемые документы, содержащие инструкции для сотрудников организации, необходимые к исполнению;
- информационные системы управления – является совокупностью организационных, технических, программных и информационных средств, которые объединены в единую систему с целью сбора, хранения, обработки и выдачи информации, которая предназначена для выполнения функций управления;
- интеллектуальные системы – это техническая или программная система, способная решать задачи, традиционно считающиеся творческими,

принадлежащие конкретной предметной области, знания о которой хранятся в памяти такой системы;

- системы автоматизации научных исследований – это программно-аппаратный комплекс на базе средств вычислительной техники, предназначенный для проведения научных исследований или комплексных испытаний образцов новой техники на основе получения и использования моделей исследуемых объектов, явлений и процессов;
- геоинформационные системы – система сбора, хранения, анализа и графической визуализации пространственных (географических) данных и связанной с ними информации о необходимых объектах [8].

Описание современных информационных систем:

1) «1С:Зарплата и управление персоналом 8» — программа массового назначения, позволяющая в комплексе автоматизировать задачи, связанные с расчетом заработной платы персонала и реализацией кадровой политики, с учетом требований законодательства и реальной практики работы предприятий. Она может успешно применяться в службах управления персоналом и бухгалтериях предприятий, а также в других подразделениях, заинтересованных в эффективной организации работы сотрудников, для управления человеческими ресурсами коммерческих предприятий различного масштаба.В «1С:Зарплате и управлении персоналом 8» поддерживаются все основные процессы управления персоналом, а также процессы кадрового учета, расчета зарплаты, планирования расходов на оплату труда, исчисления НДФЛ и страховых взносов.

2) «1С:Общеобразовательное учреждение» обеспечивает реализацию таких актуальных направлений информатизации школ, как ведение электронных классных журналов и дневников учащихся, информирование родителей об успеваемости и посещаемости их детей, учет платных образовательных услуг, управление учебным процессом в соответствии с требованиями Федеральных государственных образовательных стандартов нового поколения и многое другое.

3) «1С:Бухгалтерия8» — это самая популярная бухгалтерская программа, способная вывести автоматизацию учета на качественно новый уровень. Удобный продукт и подключаемые к нему сервисы позволят эффективно решать задачи бухгалтерской службы любого бизнеса. Фирма «1С» непрерывно совершенствует программу и сервисы, чтобы предложить современное и универсальное решение для бухгалтерии, соответствующее потребностям и задачам пользователей.«1С:Бухгалтерия 8» — это профессиональный инструмент бухгалтера, с помощью которого можно вести бухгалтерский и налоговый учет, готовить и сдавать обязательную отчетность. Программа объединила в себе все достижения предыдущих версий и новые решения, основанные на опыте практической работы бухгалтеров сотен тысяч предприятий и организаций.

Функциональные возможности«1С:Зарплата и управление персоналом 8»:

- расчет заработной платы;
- исчисление регламентированных законодательством налогов и взносов с фонда оплаты труда;
- отражение начисленной зарплаты и налогов в затратах предприятия;

- управление денежными расчетами с персоналом, включая депонирование;
- учет кадров и анализ кадрового состава; автоматизация кадрового делопроизводства.

Функциональные возможности«1С: Библиотеки ПРОФ» обеспечивает выполнение рабочих процессов библиотеки:

- комплектование;
- каталогизацию и ведение электронного каталога;
- ведение сводных каталогов объединения библиотек;
- учет, актуализацию и хранение фондов;
- обслуживание читателей;
- поддержку электронного библиотечного фонд.

Функциональные возможности «1С:Бухгалтерия 8»:

- ведение учета: любые виды, включая складской, кадровый, зарплатный и другие.
- формирование отчетности для федеральной налоговой службы и других учреждений.
- ведение информационных баз для одной или нескольких организаций.
- создание документов: счетов, актов, договоров, ордеров и других.
- подготовка первичной документации, регистрация хозяйственных операций.

Была составлена таблица отличий между информационными системами. Указаны их индивидуальные особенности, различающиеся количественные и качественные характеристики, она показана как таблица 3.

Таблица 2 – Характеристики информационных систем

Характеристики	1С:Зарплата и управление персоналом 8	1С:Комплексная автоматизация	1С:Бухгалтерия 8
Стоимость	22 600 руб.	30 000 руб.	5 400 руб.
Платформа	Microsoft, Windows, Linux, Android, Mac OS, iOS	Microsoft, Windows, Linux, Android, Mac OS, iOS	Microsoft, Windows, Linux, Android, Mac OS, iOS

Продолжение таблицы 2

Функциональность	«1С:Зарплата и управление персоналом 8 позволяет построить комплексную систему эффективного управления человеческими ресурсами компании любой численности.	«1С:Общеобразовательное учреждение» предназначена для комплексной автоматизации административно-хозяйственной деятельности, а также формирования и передачи отчетности в вышестоящие органы, в том числе в электронном виде.	Конфигурация «Бухгалтерия предприятия» предназначена для автоматизации бухгалтерского и налогового учёта, включая подготовку обязательной (регламентированной) отчётности в организации. Бухгалтерский и налоговый учёт ведётся в соответствии с действующим законодательством Российской Федерации.
Настройка	Основные настройки уже сформированы, и для того, чтобы начать вести бухучет в 1С, достаточно выбрать используемую систему налогообложения и внести данные при формировании базы	Основные настройки уже сформированы, достаточно выбрать используемую систему и внести данные при формировании базы	Основные настройки уже сформированы, и для того, чтобы начать вести бухучет в 1С, достаточно выбрать используемую систему налогообложения и внести данные при формировании базы

Продолжение таблицы 2

Характеристики	1С:Зарплата и управление персоналом 8	1С:Комплексная автоматизация	1С:Бухгалтерия 8
Поддерживаемые браузеры	Google Chrome, Mozilla Firefox, Microsoft Edge, Safari, Yandex, Microsoft Internet Explorer	Google Chrome, Mozilla Firefox, Microsoft Edge, Safari, Yandex, Microsoft Internet Explorer	Google Chrome, Mozilla Firefox, Microsoft Edge, Safari, Yandex, Microsoft Internet Explorer

Описание роли информационных систем с точки зрения повышения эффективности работы объекта автоматизации (организации, предприятия).

В современных условиях организация не может существовать и развиваться без высокоэффективной системы управления, базирующейся на самых современных информационных технологиях. Постоянно изменяющиеся требования рынка, огромные потоки информации научно-технического, технологического и маркетингового характера требуют от персонала предприятия, отвечающего за стратегию и тактику развития высокотехнологического предприятия быстроты и точности принимаемых решений, направленных на получение максимальной прибыли при минимальных издержках..

2.4 Проектирование локальной сети предприятия

Компьютерная сеть – это взаимосвязанные вычислительные устройства, которые могут обмениваться данными и совместно использовать ресурсы. Эти сетевые устройства используют систему правил, называемых коммуникационными протоколами, для передачи информации посредством физических или беспроводных технологий. Компьютерная сеть организации «Библиотека» показана на 3 рисунке.

Компьютерные сети подразделяются на три основных класса:

- глобальная вычислительная сеть (WAN - Wide Area Network) объединяет абонентов, расположенных в различных странах, на разных континентах. Взаимодействие между абонентами такой сети осуществляется на базе телефонных линий связи, радиосвязи и систем спутниковой связи;
- региональна1я вычислительная сеть (MAN - Metropolitan Area Network) связывает абонентов внутри большого города, экономического региона, страны. Обычно расстояние между абонентами региональной вычислительной сети составляет десятки - сотни километров;
- локальная вычислительная сеть (LAN – Local Area Network) включает абонентов, расположенных в пределах небольшой территории.

К классу локальных вычислительных сетей относятся сети отдельных предприятий, фирм, банков и т.д. Протяженность такой сети обычно ограничена пределами 2 – 2,5 километра [10].

Основное назначение компьютерных сетей - обеспечить совместный доступ пользователей к информации (базам данных, документам и т. д.) и ресурсам (жесткие диски, принтеры, накопители CD-ROM, модемы, выход в глобальную сеть и т. д.).

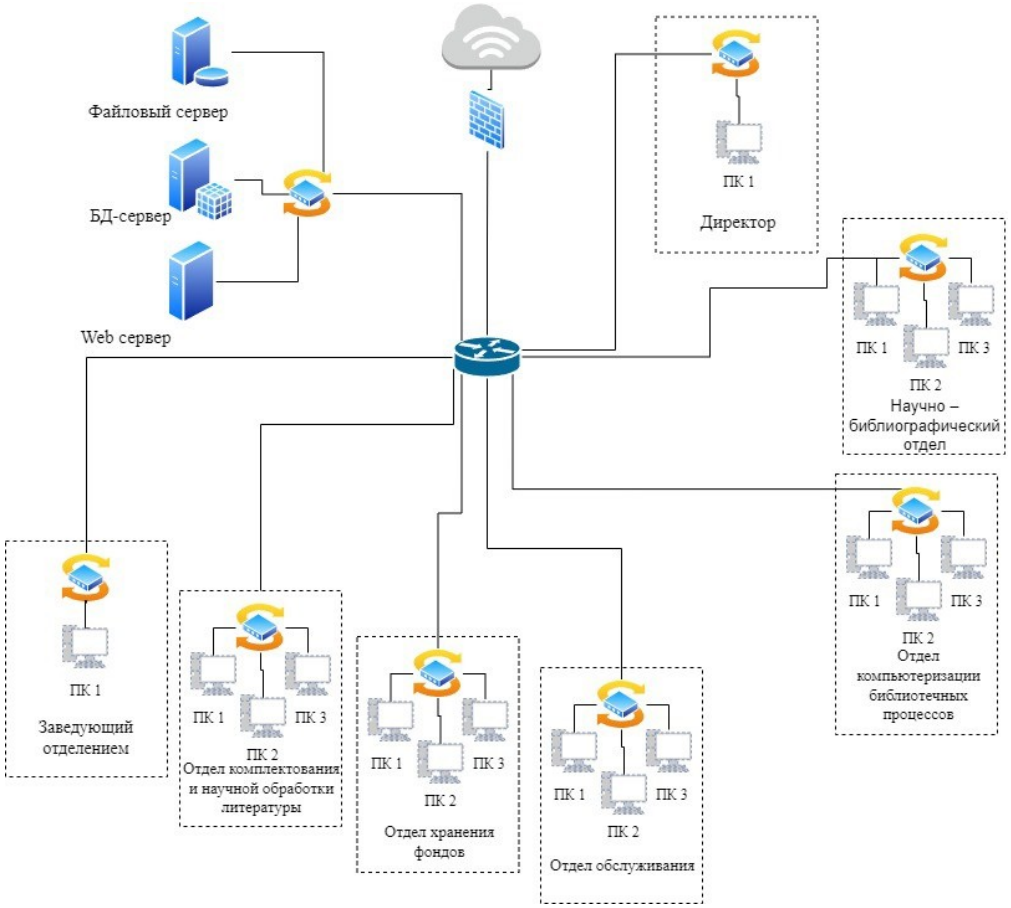


Рисунок 3 – Схема сети предприятия

Таблица 3 – Перечень ПО и технических средств объекта исследования

Наименование	Месторасположение	Фирма-изготовитель
Программное обеспечение сервера		
Microsoft Windows Server 2008 R2	Серверные	Microsoft
Программное обеспечение АРМ информационных систем		
Microsoft Windows 10	Все ПК организации	Microsoft

Продолжение таблицы 3

Наименование	Месторасположение	Фирма-изготовитель
Microsoft Office 2007/ 2010	Все ПК организации	Microsoft
Kaspersky Endpoint Security	Все ПК организации	Kaspersky
Oracle VM VirtualBox	Все ПК организации	Oracle
СБИС Управление персоналом	Отдел по личному составу	СБИС
1С:Документооборот государственного учреждения	Все отделы	1С
1С:Бухгалтерия государственного учреждения 8 ПРОФ	Бухгалтерия	1С
Технические средства информационных систем		
Рабочие станции пользователей информационной системы	Все ПК Организации	-
Сетевые кабели, соединяющие рабочие станции, сервер и модем	Помещения и коридор Организации	NETLAN
Принтеры (локальные) и прочие печатающие устройства	Во всех отделах организации	HP
Маршрутизаторы	Во всех отделах организации	ОАО QTECH
Коммутатор сети	Во всех отделах организации	Huawei
Сервера	Серверные	Intel

КС необходимо защищать, чтобы избежать утечки информации на предприятии.

3 Порядок аттестации объекта информатизации

Аттестация объекта информатизации – это комплекс организационно-технических мероприятий, в результате которых посредством специального документа – «Аттестата соответствия» подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных ФСТЭК России.

Нормативно правовая база для проведения аттестации объекта информатизации на соответствие требованиям по защите информации:

- приказ ФСТЭК России от 11 февраля 2013 г. N 17- Настоящие Требования разработаны в соответствии с Федеральным законом от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» (Собрание законодательства Российской Федерации, 2006, N 31, ст. 3448; 2010, N 31, ст. 4196; 2011, N 15, ст. 2038; N 30, ст. 4600; 2012, N 31, ст. 4328), а также с учетом национальных стандартов Российской Федерации в области защиты информации и в области создания автоматизированных систем (далее - национальные стандарты);
- приказом ФСТЭК России от 23 марта 2017 г. N 31 - В настоящем документе устанавливаются требования к обеспечению защиты информации, обработка которой осуществляется автоматизированными системами управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды (далее - автоматизированные системы управления), от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также иных неправомерных действий в отношении такой информации, в том числе от деструктивных информационных воздействий (компьютерных атак), следствием которых может стать нарушение функционирования автоматизированной системы управления.

Обязательной аттестации подлежат объекты информатизации, предназначенные для обработки информации, составляющей государственную тайну, управления экологически опасными объектами, ведения секретных переговоров. В остальных случаях аттестация носит добровольный характер (добровольная аттестация) и может осуществляться по желанию заказчика или владельца объекта информатизации [14].

Газпром Нефть подлежит обязательной аттестации, так как в организации ведутся важные переговоры, имеются секретные документы, а так же есть коммерческая тайна.

Аттестат соответствия – это документ, которым орган по сертификации удостоверяет соответствие выпускаемой в обращение продукции требованиям одного или нескольких технических регламентов Евразийского экономического союза.

Порядок проведения аттестации объектов информатизации по требованиям безопасности информации включает следующие действия:

- подачу и рассмотрение заявки на аттестацию;
- предварительное ознакомление с аттестуемым объектом;
- испытание несертифицированных средств и систем защиты информации, используемых на аттестуемом объекте (при необходимости).

Аттестация производится в порядке, установленном «Положением по аттестации объектов информатизации по требованиям безопасности информации» от 25 ноября 1994 года. Аттестация должна проводится до начала обработки информации, подлежащей защите. Это необходимо в целях официального подтверждения эффективности используемых мер и средств по защите этой информации на конкретном объекте информатизации.

Аттестация является обязательной в следующих случаях:

- государственная тайна;
- при защите государственного информационного ресурса;
- управление экологически опасными объектами;
- ведение секретных переговоров.

Аттестация предполагает комплексную проверку (аттестационные испытания) объекта информатизации в реальных условиях эксплуатации. Целью является проверка соответствия применяемых средств и мер защиты требуемому уровню безопасности. К проверяемым требованиям относится:

- защита от НСД, в том числе компьютерных вирусов;
- защита от утечки через ПЭМИН;
- защита от утечки или воздействия на информацию за счет специальных устройств, встроенных в объект информатизации.

Аттестация проводится органом по аттестации в соответствии со схемой, выбираемой этим органом, и состоит из следующего перечня работ:

- анализ исходных данных по аттестуемому объекту информатизации;
- предварительное ознакомление с аттестуемым объектом информатизации;
- проведение экспертного обследования объекта информатизации и анализ разработанной документации по защите информации на этом объекте с точки зрения ее соответствия требованиям нормативной и методической документации;
- проведение испытаний отдельных средств и систем защиты информации на аттестуемом объекте информатизации с помощью специальной контрольной аппаратуры и тестовых средств;
- проведение испытаний отдельных средств и систем защиты информации в испытательных центрах (лабораториях) по сертификации средств защиты информации по требованиям безопасности информации;
- проведение комплексных аттестационных испытаний объекта информатизации в реальных условиях эксплуатации;
- анализ результатов экспертного обследования и комплексных аттестационных испытаний объекта информатизации и утверждение заключения по результатам аттестации.

Органы по аттестации должны проходить аккредитацию ФСТЭК в соответствии с «Положением об аккредитации испытательных лабораторий и органов по сертификации средств защиты информации по требованиям безопасности информации».

Все расходы по проведению аттестации возлагаются на заказчика, как в случае добровольной, так и обязательной аттестации.

Органы по аттестации несут ответственность за выполнение своих функций, за сохранение в секрете информации, полученной в ходе аттестации, а также за соблюдение авторских прав заказчика [15].

В структуру системы аттестации входят:

- федеральный орган по сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации ФСТЭК России;
- органы по аттестации объектов информатизации по требованиям безопасности информации;
- испытательные центры (лаборатории) по сертификации продукции по требованиям безопасности информации;
- заявители (заказчики, владельцы, разработчики аттестуемых объектов информатизации).

В качестве заявителей могут выступать заказчики, владельцы или разработчики аттестуемых объектов информатизации.

Аттестат соответствия информационной системы выдается на неограниченный срок. Причем действие аттестата прекращается досрочно при изменении условий функционирования информационной системы и технологии обработки защищаемой информации.

Документация, предоставляемая органу по аттестации:

- заявление об обработке персональных данных отдельных категорий лиц, принимаемых на работу, непосредственно связанную с обеспечением транспортной безопасности, или выполняющих такую работу, проведению аттестации сил обеспечения транспортной безопасности которых предшествует обработка персональных данных;
- заявление о проведении аттестации сил обеспечения транспортной безопасности;
- анкета;
- четыре цветные фотографии аттестуемого лица размером 3х4 сантиметра, в том числе в электронном виде;
- копия документа, удостоверяющего личность аттестуемого лица, заверенная субъектом транспортной инфраструктуры, специализированной организацией в области обеспечения транспортной безопасности, организацией, претендующей на аккредитацию для проведения оценки уязвимости объектов транспортной инфраструктуры и транспортных средств, подразделением транспортной безопасности, организацией, претендующей на аккредитацию в качестве подразделения транспортной безопасности;

- копия трудовой книжки аттестуемого лица, заверенная надлежащим образом субъектом транспортной инфраструктуры, подразделением транспортной безопасности, организацией, претендующей на аккредитацию в качестве подразделения транспортной безопасности, и (или) сведения о трудовой деятельности, за исключением случаев, когда трудовая (служебная) деятельность ранее не осуществлялась;

- копия документа (документов) об образовании аттестуемого лица, заверенная субъектом транспортной инфраструктуры, специализированной организацией в области обеспечения транспортной безопасности, организацией, претендующей на аккредитацию для проведения оценки уязвимости объектов транспортной инфраструктуры и транспортных средств, подразделением транспортной безопасности, организацией, претендующей на аккредитацию в качестве подразделения транспортной безопасности;

- справка о наличии (отсутствии) судимости и (или) факта уголовного преследования либо о прекращении уголовного преследования в отношении аттестуемого лица, выданная не ранее 60 дней до дня представления этой справки;

- справка, выданная соответствующей медицинской организацией не ранее 60 дней до дня представления этой справки, подтверждающая отсутствие психических заболеваний, алкоголизма, наркомании, токсикомании и отсутствие диспансерного наблюдения в отношении указанных заболеваний в связи с выздоровлением или стойкой ремиссией, являющихся ограничением при выполнении работ, непосредственно связанных с обеспечением транспортной безопасности;

- справка о том, является или не является лицо подвергнутым административному наказанию за потребление наркотических средств или психотропных веществ без назначения врача либо новых потенциально опасных психоактивных веществ, выданная не ранее 60 дней до дня представления этой справки;

- копия свидетельства об аттестации сил обеспечения транспортной безопасности, заверенная субъектом транспортной инфраструктуры, специализированной организацией в области обеспечения транспортной безопасности, организацией, претендующей на аккредитацию для проведения оценки уязвимости объектов транспортной инфраструктуры и транспортных средств, подразделением транспортной безопасности, организацией, претендующей на аккредитацию в качестве подразделения транспортной безопасности (в случае его наличия);

Документация, предоставляемая органу по аттестации:

- состав аттестационной комиссии (группы);

- дата проведения аттестации;

- перечень руководящих документов, в соответствии с которыми проводилась аттестация;

- перечень документов по защите информации в выделенном помещении, представленных аттестационной комиссии;

- характеристику выделенного помещения (назначение, местоположение, условия размещения и т.д.);
- перечень вспомогательных технических средств и систем (ВТСС), установленных на объекте информатизации;
- перечень технических средств защиты информации, установленных в выделенном помещении;
- характеристику организационных мероприятий по защите информации;
- виды работ, проводимых в ходе аттестации;

Содержание протокола аттестационных испытаний помещения:

- вид испытаний;
- объект испытаний;
- дату и время проведения испытаний;
- место проведения испытаний;
- перечень использованной в ходе испытаний аппаратуры (наименование, тип, заводской номер, номер свидетельства о поверке и срок его действия);
- перечень нормативно-методических документов, в соответствии с которыми проводились испытания;
- методику проведения испытания (краткое описание);
- результаты измерений;
- результаты расчетов.

Содержание аттестата соответствия на объект информатизации:

- регистрационный номер;
- дату выдачи;
- срок действия;
- наименование, адрес и местоположение объекта информатизации;
- категорию объекта информатизации;
- класс защищенности автоматизированной системы;
- гриф секретности (конфиденциальности) информации, обрабатываемой на объекте информатизации.

Владелец аттестованного объекта информатизации несет ответственность за выполнение установленных условий функционирования объекта информатизации , технологии обработки защищаемой информации и требований по безопасности информации.

В случае изменения условий и технологии обработки защищаемой информации владельцы аттестованных объектов обязаны известить об этом Управление и орган по аттестации, проводивший аттестацию объекта информатизации.

4 Анализ защищенности объекта информатизации

4.1 Построение модели нарушителя

Нарушитель – это лицо, совершившее или пытающееся совершить несанкционированное действие, а также лицо, оказывающее ему содействие в этом.

Злоумышленник – это человек, совершивший преступление, которое он заранее задумал.

Злоумышленник отличается от нарушителя, тем что он совершает преступление намеренно, обдумывая его заранее, а нарушитель может совершить преступление случайно.

Модель нарушителя – предположения о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности» [13].

Рассмотрим кто будет ответственным за обеспечение защиты информации, характеристику систем и сетей как объекта защиты, взаимодействие с системами других организация и технологии используемые организации «Библиотека».

Таблица 4 – Ответственность за обеспечение защиты информации

№	Роль подразделения (должностного лица)	Должностное лицо, подразделение
1	Ответственный за обеспечения безопасности ПДн и за защиту информации, не содержащей сведения составляющих государственную тайну	Начальник отдела ИТ
2	Ответственный за планирование и контроль мероприятий по обеспечению ИБ	Специалист по обеспечению информационной безопасности

Продолжение таблицы 4

№	Роль подразделения (должностного лица)	Должностное лицо, подразделение
3	Ответственный за управление (администрирования) системы защиты информации (подсистемы безопасности)	Системный администратор
4	Ответственный за выявление компьютерных инцидентов и реагирование на них	Специалист по обеспечению информационной безопасности
5	Сотрудник, которому разрешены действия по внесению изменений в конфигурации	Специалист по обеспечению защиты информации
6	Администратор безопасности значимого объекта	Системный администратор
7	Структурное подразделение, осуществляющее функции по обеспечению ИБ	Отдел ИБ

Таблица 5 - Описание систем и сетей их характеристика как объекта защиты

№	Характеристики	Значение характеристик
1	Программно-аппаратные средства	Внешние аппаратные устройства (клавиатура, мышь, принтеры), информационные системы организации, базы данных, автоматизированные системы.
2	Общее системное ПО	Операционные системы Windows 10
3	Прикладное ПО	Набор прикладных программ MicrosoftOffice, электронные таблицы, графические редакторы, ПО для воспроизведения мультимедийных данных.
4	Средства защиты информации	Антивирус Kaspersky

Таблица 6 - Взаимодействие с системами других организаций

Наименование системы	Тип системы	Цель взаимодействия	Характеристики взаимодействий	Передаваемая информация
Банки России	Экономическая	Получение услуг	Получение услуг	Персональные данные сотрудников и клиентов
Кадровое агентство	Социальная	Сотрудничество	Получение новых кадров	Персональные данные
ФСТЭК	Правовая	Получение услуг	Передача информации	Нормативно-правовые акты

Таблица 7 - Технологии используемые на предприятии

№	Технология	Используется/Не используется
1	Съемные носители информации	Используется
2	Технологии виртуализации	Не используется
3	Технологии беспроводного доступа	Используется
4	Мобильные технические средства	Не используется
5	Веб серверы	Используется
6	Технология веб доступа	Используется
7	Смарт-карты	Не используется
8	Технология грид-систем	Не используется
9	Технология суперкомпьютерных систем	Не используется
10	Большие данные	Используется
11	Числовое программное оборудование	Не используется
12	Одноразовые пароли	Не используется
13	Электронная почта	Используется
14	Технология передачи видеоинформации	Используется
15	Технология удаленного рабочего стола	Не используется
16	Т. Удаленного администрирования	Используется
17	Т. Удаленного доступа	Используется
18	Т. Передачи речи	Используется
19	Т. ИИ	Не используется

Таблица 8 – Возможные негативные последствия от реализации угроз безопасности информации

Идентификатор	Негативные последствия(НП)	Виды риска(ущерб)
НП1	Принятие неправильных решений	У3
НП.2	Разглашение персональных данных граждан	У1
НП.3	Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.)	У3
НП.4	Нарушение неприкосновенности частной жизни	У1
НП.5	Нарушение личной, семейной тайны, утрата чести и доброго имени	У1
НП.6	Нарушение иных прав и свобод гражданина, закрепленных в Конституции Российской Федерации и федеральных законах	У1
НП.7	Нарушение кониденциальности (утечка) персональных данных	У1
НП.8	Нарушение законодательства Российской Федерации (юридическое лицо, индивидуальный предприниматель)	У2
НП.9	Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций	У2
НП.10	Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств)	У2
НП.11	Потеря клиентов, поставщиков	У3
НП.13	Нарушение деловой репутации	У3
НП.14	Утрата доверия	У3
НП.15	Утечка информации ограниченного доступа	У3
НП.16	Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций)	У2

У1 – ущерб физическому лицу.

У2 – Риски юридическому лицу, ИП связанные с хоз. деятельностью.

У3 – Ущерб государству в области обороны страны, безопасности государства и правопорядка, а также социальный, экономической, политической, экологической сферах деятельности.

Возможные объекты воздействия угроз безопасности информации приведены в таблице 9.

Таблица 9 – Виды воздействия

Идентификатор	Вид воздействия
ВВ.1	утечка (перехват) конфиденциальной информации или отдельных данных (нарушение конфиденциальности)
ВВ.2	несанкционированный доступ к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данным
ВВ.3	отказ в обслуживании компонентов (нарушение доступности)
ВВ.4	несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных служебных данных (нарушение целостности)
ВВ.5	несанкционированное использование вычислительных ресурсов систем и сетей в интересах решения несвойственных им задач
ВВ.6	нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передачи и хранения информации

Таблица 10 – Объекты и виды воздействия

Негативные последствия	Объекты воздействия	Виды воздействия
утечка (перехват) конфиденциальной информации или отдельных данных (нарушение конфиденциальности)	конфиденциальная информация	ВВ.1
несанкционированный доступ к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данным	компоненты, защищаемой информации, системным, конфигурационным, иным служебным данным	ВВ.2

Продолжение таблицы 10

Негативные последствия	Объекты воздействия	Виды воздействия
отказ в обслуживании компонентов (нарушение доступности)	обслуживание компонентов	ВВ.3
несанкционированная моификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных служебных данных (нарушение целостности)	Защищаемая информация, системных, конфигурационных, иных служебных данных	ВВ.4
несанкционированное использование вычислительных ресурсов систем и сетей в интересах решения несвойственных им задач	Вычислительные ресурсы систем и сетей	ВВ.5
нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передачи и хранения информации	программно-аппаратные средства обработки, передачи и хранения информации	ВВ.6

Таблица 11 – Перечень рассматриваемых нарушителей

№	Вид нарушителя	Возможные цели реализации угроз безопасности информации	Предложения по отнесению к числу потенциальных нарушителей
1	Специальные службы иностранных государств	Нанесение ущерба государству в области обеспечения обороны, безопасности и правопорядка, а также в иных отдельных областях его деятельности или секторах экономики, в том числе дискредитация или дестабилизация деятельности отдельных органов государственной власти, организаций, получение конкурентных преимуществ на уровне государства, срыв заключения международных договоров, создание внутриполитического кризиса	Не являются
2	Террористические, экстремистские группировки	Совершение террористических актов, угроза жизни граждан. Нанесение ущерба отдельным сферам деятельности или секторамэкономики государства. Дестабилизация общества. Дестабилизация деятельности органов государственной власти, организаций	являются
3	Преступные группы (криминальные структуры)	Получение финансовой или иной материальной выгоды. Желание самореализации (подтверждение статуса)	Не являются

Продолжение таблицы 11

№	Вид нарушителя	Возможные цели реализации угроз безопасности информации	Предложения по отнесению к числу потенциальных нарушителей
4	Отдельные физические лица (хакеры)	Получение финансовой или иной материальной выгоды. Любопытство или желание самореализации (подтверждение статуса)	являются
5	Конкурирующие организации.	Получение конкурентных преимуществ. Получение финансовой или иной материальной выгоды	Не являются
6	Разработчики программных, программно-аппаратных средств	Внедрение дополнительных функциональных возможностей в программные или программно-аппаратные средства на этапе разработки. Получение конкурентных преимуществ. Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия	являются

Продолжение таблицы 11

№	Вид нарушителя	Возможные цели реализации угроз безопасности информации	Предложения по отнесению к числу потенциальных нарушителей
7	Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия. Получение конкурентных преимуществ	являются
8	Поставщики вычислительных услуг, услуг связи	Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия. Получение конкурентных преимуществ	являются
9	Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия. Получение конкурентных преимуществ	Не являются
10	Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.)	Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия	являются

Продолжение таблицы 11

№	Вид нарушителя	Возможные цели реализации угроз безопасности информации	Предложения по отнесению к числу потенциальных нарушителей
1 1	Авторизованные пользователи систем и сетей	Получение финансовой или иной материальной выгоды. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия	являются
1 2	Системные администраторы и администраторы безопасности	Получение финансовой или иной материальной выгоды. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия	являются
1 3	Бывшие работники (пользователи)	Получение финансовой или иной материальной выгоды. Месть за ранее совершенные действия	являются

Характеристики возможных нарушителей описаны в таблице 13, где:

- Н1 - нарушитель который имеет возможность реализовывать только известные угрозы, направленные на известные (документированные) уязвимости с использованием обще доступных инструментов;

- Н2 - нарушитель который имеет возможность реализовывать угрозы в том числе направленные на неизвестные (недокументированные) уязвимости с использованием специально созданных для этого инструментов свободно распространяемых в интернете. Не имеет возможности реализации угроз на физически изолированные сегменты сетей и систем;

- Н3 - нарушитель который имеет возможность реализовывать угрозы в том числе на выявленные им неизвестные уязвимости с использованием

самостоятельно разработанных для этого инструментами. Не имеет возможности реализации угроз на физически изолированные сегменты сетей и систем;

- Н4 - нарушитель, имеющий практически не ограниченные возможности в том числе незадекларированных возможностей программных программно-аппаратных закладок встроенных в компоненты сетей.

Таблица 12– Характеристики возможных нарушителей

№	Возможный вид нарушителя	Категория	Уровень возможностей	Актуальность
1	Специальные службы иностранных государств	Внешний	Н4	Нет
2	Террористические, экстремистские группировки	Внешний	Н1	Нет
3	Преступные группы (криминальные структуры)	Внешний	Н1	Нет
4	Отдельные физические лица (хакеры)	Внешний	Н4	Да
5	Конкурирующие организации.	Внешний	Н2	Нет
6	Разработчики программных, программно-аппаратных средств	Внешний	Н3	Нет
7	Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Внешний	Н2	Нет
8	Поставщики вычислительных услуг, услуг связи	Внешний	Н3	Нет
9	Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Внутренний	Н3	Нет

Продолжение таблицы 12

№	Возможный вид нарушителя	Категория	Уровень возможностей	Актуальность
10	Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.)	Внутренний	Н3	Нет
11	Авторизованные пользователи систем и сетей	Внутренний	Н2	Да
12	Системные администраторы и администраторы безопасности	Внутренний	Н3	Да
13	Бывшие работники	Внешние	Н1	Нет

Уровень возможностей:

- Н1 – нарушитель обладающий базовыми возможностями;
- Н2 - нарушитель обладающий базовыми повышенными возможностями;
- Н3 - нарушитель обладающий средними возможностями;
- Н4 - нарушитель обладающий высокими возможностями.

Н1– нарушитель который имеет возможность реализовывать только известные угрозы направленные на известные (документированные) уязвимости с использованием обще доступных инструментов.

Н2 – нарушитель который имеет возможность реализовывать угрозы в том числе направленные на неизвестные (недокументированные) уязвимости с использованием специально созданных для этого инструментов свободно распространяемых в интернете. Не имеет возможности реализации угроз на физически изолированные сегменты сетей и систем.

Н3 – нарушитель который имеет возможность реализовывать угрозы в том числе на выявленные им неизвестные уязвимости с использованием самостоятельно разработанных для этого инструментами. Не имеет возможности реализации угроз на физически изолированные сегменты сетей и систем.

Н4 – нарушитель, имеющий практически не ограниченные возможности в том числе недиклорированных возможностей программных программно-аппаратных закладок встроенных в компоненты сетей.

Таблица 13 – Перечень возможных способов реализации угроз безопасности информации

Идентификатор	Способы реализации
СР.1	Использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей, а также организационных и многофакторных уязвимостей)
СР.2	Внедрение вредоносного программного обеспечения
СР.3	Использование недекларированных возможностей программного обеспечения и (или) программно-аппаратных средств
СР.4	установка программных и (или) программно-аппаратных закладок в программное обеспечение и (или) программно-аппаратные средства
СР.5	Формирование и использование скрытых каналов (по времени, по памяти) для передачи конфиденциальных данных
СР.6	Перехват (измерение) побочных электромагнитных излучений и наводок (других физических полей) для доступа к конфиденциальной информации, содержащейся в аппаратных средствах аутентификации
СР.7	Инвазивные способы доступа к конфиденциальной информации, содержащейся в аппаратных средствах аутентификации
СР.8	Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам (в том числе администрированию, обслуживанию)
СР.9	Ошибочные действия в ходе создания и эксплуатации систем и сетей, в том числе при установке, настройке программных и программно-аппаратных средств
СР.10	Перехват трафика сети передачи данных
СР.11	Несанкционированный физический доступ и (или) воздействие на линии, (каналы) связи, технические средства, машинные носители информации
СР.12	Реализация атак типа «отказ в обслуживании» в отношении технических средств, программного обеспечения и каналов передачи данных

Таблица 14 – Определение актуальных способов реализации угроз безопасности информации и соответствующим им виды нарушителей и их возможности

N п/п	Вид нарушителя	Категория нарушителя	Объект воздействия	Доступные интерфейсы	Способы реализации
1	Отдельные физические лица (хакеры)	Внешний	База данных информационной системы, содержащая идентификационную информацию граждан: несанкционированный доступ к компонентам систем или сетей, защищаемой информации, системным, конфигурационным, иным служебным данным; утечка (нарушение конфиденциальности) защищаемой информации, системных, конфигурационных, иных служебных данных	Веб-интерфейс удаленного администрирования базы данных информационной системы	Использование недекларированных возможностей программного обеспечения телекоммуникационного оборудования
				Пользовательский веб-интерфейс доступа к базе данных информационной системы	Использование уязвимостей конфигурации системы управления базами данных
			Линия связи между сервером основного центра обработки данных и сервером резервного центра обработки данных: перехват (нарушение конфиденциальности) защищаемой информации,	Канал передачи данных между сервером основного центра обработки данных и сервером резервного центра обработки данных	Установка программных закладок в телекоммуникационное оборудование

Продолжение таблицы 14

N п/п	Вид нарушителя	Категория нарушителя	Объект воздействия	Доступные интерфейсы	Способы реализации
			системных, конфигурационных, иных служебных данных		
2	Авторизованные пользователи систем и сетей	Внутренний	АРМ главного бухгалтера организации: модификация платежных поручений, хранящихся на АРМ главного бухгалтера	ЛВС организации	Ошибочные действия в ходе настройки АРМ главного бухгалтера
				Съемные машинные носители информации, подключаемые к АРМ пользователя	Использование уязвимостей конфигурации системы управления доступом к АРМ пользователя
3	Системные администраторы и администраторы безопасности	Внутренний	База данных ИС, содержащая идентификационную информацию клиентов и сотрудников	Веб-интерфейс удаленного администрирования базы данных ИС	Использование недекларированных возможностей программного обеспечения и (или) программно-аппаратных средств
			Линия связи между сервером основного центра обработки данных и сервером резервного центра обработки данных: перехват защищаемой информации, системных, конфигурационных, иных служебных данных	Канал передачи данных между сервером основного центра обработки данных и сервером резервного центра обработки данных	Установка программных и программно-аппаратных закладок в программное обеспечение и программно-аппаратные

Оценка угроз в соответствии с методическими документами ФСБ РФ.

Угроза информации – это потенциально существующая опасность случайного или преднамеренного разрушения, несанкционированного получения или модификации данных, обусловленная структурой системы обработки, а также условиями обработки и хранения данных.

Модель угроз строится на основе методического документа «Методика оценки угроз безопасности информации» ФСТЭК [18].

Рассмотрим актуальные угрозы в организации «Библиотека».

Таблица 15 – Результирующая модель угроз

Идентификатор угрозы	Наименование угрозы
УБИ.008	Угроза восстановления и/или повторного использования аутентификационной информации
УБИ.028	Угроза использования альтернативных путей доступа к ресурсам
УБИ.071	Угроза несанкционированного восстановления удалённой защищаемой информации
УБИ.074	Угроза несанкционированного доступа к аутентификационной информации
УБИ.091	Угроза несанкционированного удаления защищаемой информации
УБИ.198	Угроза скрытной регистрации вредоносной программой учетных записей администраторов
УБИ.205	Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты
УБИ.209	Угроза несанкционированного доступа к защищаемой памяти ядра процессора
УБИ.212	Угроза перехвата управления информационной системой
УБИ.215	Угроза несанкционированного доступа к системе при помощи сторонних сервисов

На основании методики оценки угроз от 5 февраля 2021 года, были составлены модель нарушителя, а также модель угроз предприятия.

4.2 Описание методов защиты информации в АИС

При организации автоматизированных информационных систем (АИС) должны строго соблюдаться требования по защите конфиденциальных данных, которые призваны предотвратить их утечку или искажение. Защита информации в автоматизированной системе должна предотвратить воздействие угроз различного происхождения, включая техногенные аварии, воздействие вредоносного ПО или хакеров, похищение данных инсайдерами с целью продажи или шпионажа.

Снизить уровень таких рисков позволяет реализация комплекса мер защиты аппаратного и программного уровня.

Информация имеет определенную ценность. При этом изменение ряда свойств информации может приводить к потере такой ценности.

К числу таких свойств по действующему законодательству об охране данных относятся:

- конфиденциальность — невозможность доступа третьих лиц;
- целостность (неизменность) — возможность изменения информации только лицами, которые имеют соответствующий допуск;
- доступность это – обеспечение доступа пользователя к необходимой информации без ограничений в связи с проблемами аппаратного уровня или действия вредоносного программного обеспечения.

Методы защиты информации в автоматизированных системах должны применяться ко всему массиву данных, которые обрабатываются в компании, а также по отношению к отдельным блокам повышенной важности.

При построении системы защиты информации в АИС могут применяться одновременно разные методы, в том числе:

- методы повышения уровня достоверности данных;
- методы защиты информации в автоматизированных системах от их потери в результате аварий и аппаратных сбоев;
- методы контроля физического доступа к оборудованию и сетям, который может приводить к хищению данных, повреждению аппаратуры, преднамеренному созданию нештатных и аварийных ситуаций, установке шпионских приборов;
- методы идентификации пользователей, аутентификации ПО, съемных носителей [19].

5 Проектирование защищенной компьютерной сети предприятия

5.1 Моделирование сети с помощью Cisco Packet Tracer

Программное решение Cisco Packet Tracer позволяет имитировать работу различных сетевых устройств: маршрутизаторов, коммутаторов, точек беспроводного доступа, персональных компьютеров, сетевых принтеров, IP-телефонов и т.д. Работа с интерактивным симулятором дает весьма правдоподобное ощущение настройки реальной сети, состоящей из десятков или даже сотен устройств. Настройки, в свою очередь, зависят от характера устройств: одни можно настроить с помощью команд операционной системы Cisco IOS, другие – за счет графического веб-интерфейса, третьи – через командную строку операционной системы или графические меню [20].

Основные преимущества и возможности Packet Tracer:

- усовершенствованное изображение сетевого оборудования со способностью добавлять / удалять различные компоненты;
- режим симуляции;
- возможность смоделировать логическую топологию;
- рабочее пространство для того, чтобы создать сети любого размера на CCNA-уровне сложности;
- дружественный графический интерфейс (GUI), что способствует к лучшему пониманию организации сети, принципов работы устройства;
- моделирование в режиме real-time (реального времени);
- многоязычность интерфейса программы: что позволяет изучать программу на своем родном языке;
- наличие Activity Wizard позволяет сетевым инженерам, студентам и преподавателям создавать шаблоны сетей и использовать их в дальнейшем;
- проектирование физической топологии.

Созданная схема сети объекта представлена на рисунке 4.

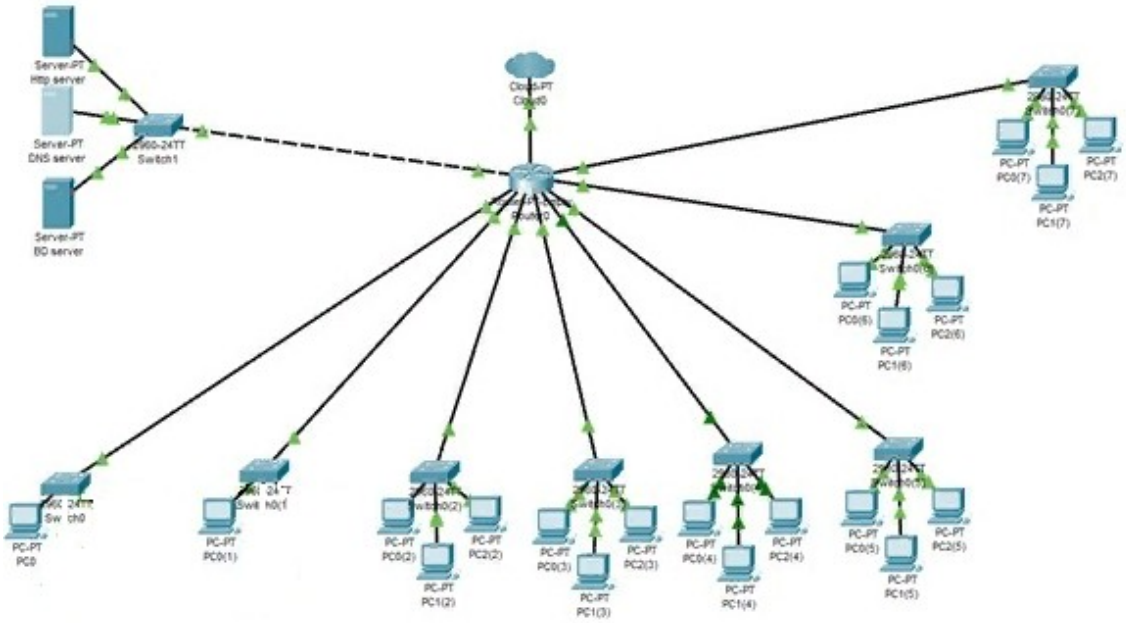


Рисунок 4 – Созданная схема сети

Для создания схемы были использованы:
- персональный компьютер (20 шт.);
- коммутатор (9 шт.);
- маршрутизатор 2811 (1 шт.);
- сервер-PT (3 шт.);
- прямой кабель (26 шт.);
- DTE кабель (1 шт.).

5.2 Настройка сетевых устройств

При создании схемы сети были настроены АРМ пользователей. Каждое АРМ, как и каждый сервер имеет:

- собственный IP-адрес;
- маску сети;
- стандартный выходной шлюз;
- DNS-сервер.

Настройка АРМ 1 представлена на рисунке 5.

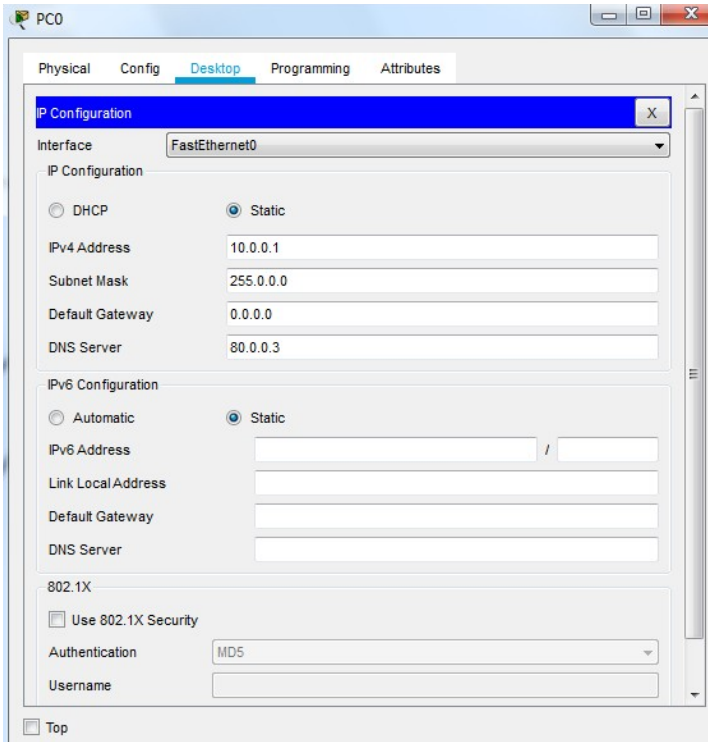


Рисунок 5 – Настройка IP АРМ

Сетевые настройки сервера представлены на рисунке 6.

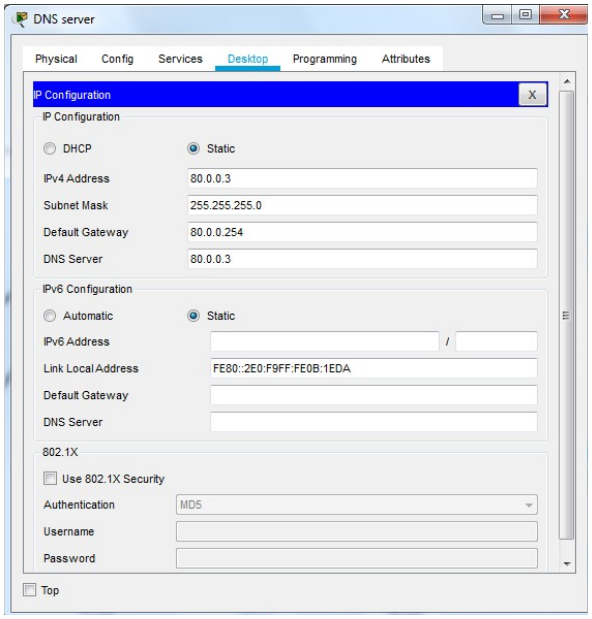


Рисунок 6 – Настройка IP сервера

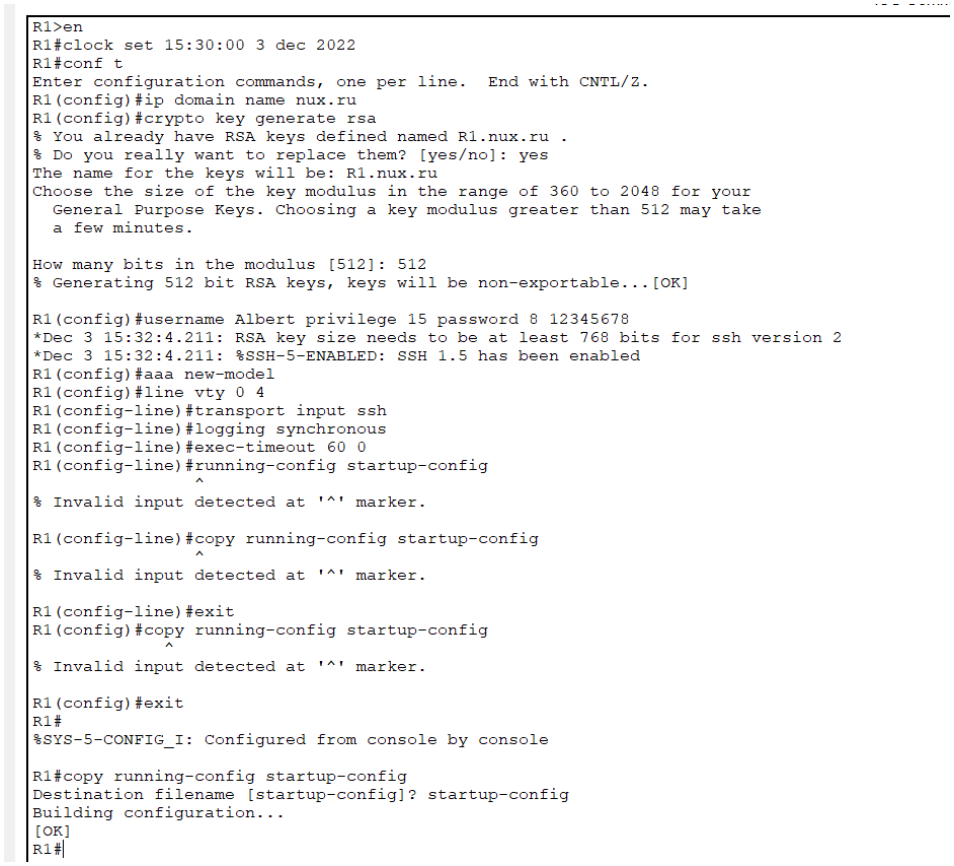
5.3 Организация системы защиты компьютерной сети предприятия

SSH – сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой и туннелирование TCP-соединений, который шифрует весь трафик, включая и передаваемые пароли [12].

Для защиты маршрутизатора необходимо:

- установить время генерации ключа;
- указать имя домена генерации ключа;
- активировать шифрование паролей в конфигурационном файле;
- создать пользователя и пароль;
- активировать протокол AAA;
- указать SSH, как среду доступа через сеть по умолчанию;
- указать время таймауту до автоматического закрытия сессии;

Организация системы защиты маршрутизатора и необходимые для этого команды представлены на рисунке 7.



```
R1>en
R1#clock set 15:30:00 3 dec 2022
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip domain name nux.ru
R1(config)#crypto key generate rsa
% You already have RSA keys defined named R1.nux.ru .
% Do you really want to replace them? [yes/no]: yes
The name for the keys will be: R1.nux.ru
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 512
% Generating 512 bit RSA keys, keys will be non-exportable...[OK]

R1(config)#username Albert privilege 15 password 8 12345678
*Dec 3 15:32:4.211: RSA key size needs to be at least 768 bits for ssh version 2
*Dec 3 15:32:4.211: %SSH-5-ENABLED: SSH 1.5 has been enabled
R1(config)#aaa new-model
R1(config)#line vty 0 4
R1(config-line)#transport input ssh
R1(config-line)#logging synchronous
R1(config-line)#exec-timeout 60 0
R1(config-line)#running-config startup-config
               ^
% Invalid input detected at '^' marker.

R1(config-line)#copy running-config startup-config
               ^
% Invalid input detected at '^' marker.

R1(config-line)#exit
R1(config)#copy running-config startup-config
           ^
% Invalid input detected at '^' marker.

R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#copy running-config startup-config
Destination filename [startup-config]? startup-config
Building configuration...
[OK]
R1#
```

Рисунок 7 – Организация системы защиты маршрутизатора

Для защиты коммутатора необходимо:

- выбрать диапазон неактивных портов;
- перевести порты в access режим;
- ограничить число адресов на интерфейсе;
- выбрать способ изучения MAC-адресов коммутатором;
- задать тип реагирования на превышение числа разрешенных MAC-адресов [1].

Организация системы защиты коммутатора и необходимые для этого команды представлены на рисунке 8.

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int range fa 0/3-24
Switch(config-if-range)#sw
Switch(config-if-range)#switchport mod
Switch(config-if-range)#switchport mode ac
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport port-security
Switch(config-if-range)#sw
Switch(config-if-range)#switchport po
Switch(config-if-range)#switchport port-security max
Switch(config-if-range)#switchport port-security maximum 4
Switch(config-if-range)#switchport port-security mac-address sticky
Switch(config-if-range)#switchport port-security violation shutdown
Switch(config-if-range)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console
```

Рисунок 8 – Организация системы защиты коммутатора

Для настройки SSH заходим в маршрутизатор и пишем команды:

Router>en

Router#clock set “время” “дата”

Router#conf t

Router(config)#ip domain name ssh.dom

Router(config)#crypto key generate rsa

Router(config)#service password-encryption

Router(config)#username “имя пользователься” privilege “уровень привилегий” password “кол-во символов в пароле” “пароль”

Router(config)#aaa new-model

Router(config)#line vty 0 4

Router(config-line)#transport input ssh

Router(config-line)#logging synchronous

Router(config-line)#exec-timeout “время таймаута до автоматического закрытия SSH сессии”

Router(config-line)#exit

Router(config)#exit

Router#copy running-config startup-config

Настройка SSH показана на рисунке 9.

```
R>en
R#clock set 21:56:23 Dec 2022
                ^
% Invalid input detected at '^' marker.

R#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R(config)#ip domain name ssh.dom
R(config)#crypto key generate rsa
% You already have RSA keys defined named R.ssh.dom .
% Do you really want to replace them? [yes/no]: yes
The name for the keys will be: R.ssh.dom
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may tak
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R(config)#service password-encryption
*Dec 6 21:3:46.620: %SSH-5-ENABLED: SSH 1.99 has been enabled
R(config)#aaa new-model
R(config)#line vty 0 4
R(config-line)#transport input ssh
R(config-line)#logging synchronous
R(config-line)#exec-timeout 60 0
R(config-line)#exit
R(config)#exit
R#
%SYS-5-CONFIG_I: Configured from console by console

R#copy running-config startup-config
Destination filename [startup-config]? startup-config
Building configuration...
[OK]
R#
```

Рисунок 9 – Настройка SSH

5.4 Тестирование работоспособности сети

Проверка работоспособности АРМ выполняется с помощью команды ping, с указанием IP-адреса назначения. Результат проверки представлен на рисунке 10.

```
C:\>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.0.2: bytes=32 time=1ms TTL=127
Reply from 10.0.0.2: bytes=32 time<1ms TTL=127
Reply from 10.0.0.2: bytes=32 time=1ms TTL=127
Reply from 10.0.0.2: bytes=32 time<1ms TTL=127

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Рисунок 10 – Проверка работоспособности сети между отделами

Для проверки работоспособности web-сервера, необходимо зайти на страницу, указанную в настройках dns (www.cisco.com). Результат проверки представлен на рисунке 11.

Рисунок 11 – Результат проверки работоспособности web-сервера

Была создана схема сети в программе Cisco Packet Tracer. Схема имеет 5 отделов, компьютерный класс, а также web-сервер. Была произведена настройка оконечных устройств они были настроены и взаимосвязаны между собой. Каждый ПК имеет доступ к web-серверу и может посетить созданный сайт «www.cisco.com». Каждый отдел имеет собственный логический (vlan) канал.

Используемые в схеме коммутаторы и маршрутизаторы были защищены и настроены.

Заключение

В результате учебной практики, были закреплены навыки и знания об автоматизированных информационных системах. Повторили их назначение и функции и рассмотрели процессы, происходящие в них.

Были выполнены задачи по изучению основных процессов, протекающих в предметной области, изучили автоматизированные информационные системы, разработали организационную структуру, рассмотрели и разработали информационные потоки.

При помощи программы Draw.io была спроектирована локальная сеть организации и создан перечень программного обеспечения и технических средств объекта исследования.

При создания схемы сети организации «Библиотека» была использована программа Cisco Packet Tracer, с помощью которой провели следующие настройки сети:

- назначение IP-адресов и маски для каждого компьютера;
- настройка коммутаторов и маршрутизаторов;
- организация связи внутри отделов и между ними;
- разработка DNS и WEB серверов организации;
- создание файлового сервера и сервера базы данных;
- настройка сетевого протокола SSH;
- создание и настройка VLAN портов для отделов;
- тестирование работоспособности модели сети.

Используя справочную правовую систему «Консультант плюс», была изучена нормативная база для проведения аттестации объекта информатизации, а так же изучение актуальных угроз.

На основании методического документа «Методика оценки угроз безопасности информации» (утв. ФСТЭК России 05.02.2021) был проведен анализ защищенности объекта информатизации, а именно определена архитектура и условия функционирования системы и сети организации. Построена модель нарушителя и модель угроз для Библиотеки, а также описаны методы защиты информации в АИС.

В ходе учебной практики были получены знания и навыки по обеспечению информационной безопасности в автоматизированных системах и компьютерных сетях. Все полученные навыки и знания пригодятся в дальнейшем при трудоустройстве на предприятие.

Список использованных источников

1 Дроздов, С.Н. Операционные системы: учебное пособие / С.Н. Дроздов. – Ростов на Дону: Феникс, – 2018. – 480 с.

2 Назаров, С.В. Операционные системы: практикум (для бакалавров) / С.В. Назаров., Л.П. Гудыно., А.А. Кириченко. – Москва: КноРус, – 2017. – 480 с.

3 Тельнова, Ю.Ф. Информационные системы и технологии / Ю.Ф. Тельнова. – Москва: Юнити, – 2017. – 544 с.

4 Бабаш, А.В. Информационная безопасность: лабораторный практикум / А.В. Бабаш., Е.К. Баранова., Ю.Н. Мельников. – Москва: КноРус, – 2019. – 432 с.

5 Баранова , Е.К. Информационная безопасность и защита информации: учебное пособие / Е.К. Баранова., А.В. Бабаш. – Москва: Риор, – 2017. – 476 с.

6 Бурко, Р.А., Соколова, В.Д. Выбор и обоснование организационной структуры предприятия / Р.А. Бурко., В.Д. Соколова. – Москва: Молодой ученый, 2019.– 315 с.

7 Баринов, В.В. Компьютерные сети: учебник / В.В. Баринов, И.В. Баринов., А.В. Пролетарский. – Москва: Academia, – 2018. – 192 с.

8 Крузин, А.В. Библиотечный форум: учебное пособие / А.В. Кузин., Д.А. Кузин. – Москва: Форум, – 2018. – 704 с.

9 Гришина, Н.В. Информационная безопасность предприятия: учебное пособие / Н.В. Гришина. – Москва.: Форум, – 2018. – 118 с.

10 Куроуз, Дж. Компьютерные сети: нисходящий подход / Дж. Куроуз. – Москва: Эксмо, – 2018. – 800 с.

11 Новожилов, Е.О. Компьютерные сети: учебное пособие / Е.О. Новожилов. – Москва: Академия,– 2018. – 176 с.

12 Таненбаум, Э. Компьютерные сети / Э. Таненбаум. – Питер: Академия, – 2019. – 960 с.

13 Щербакова, Т.Ф. Вычислительная техника и информационные технологии: учебное пособие / Т.Ф. Щербакова. – Москва: Академия, – 2017. – 128 с.

14 Мельников, В.П. Защита информации: учебник / В.П. Мельников. – Москва: Академия, – 2019. – 320 с.

15 Краковский, Ю.М. Защита информации: учебное пособие / Ю.М. Краковский. – Ростов на Дону: Феникс, – 2017. – 347 с.

16 Таненбаум, Э. Современные операционные системы / Э. Таненбаум. – Питер: Академия, – 2019. – 1120 с.

17 Матросов, В.Л. Операционные системы, сети и интернет – технологии: учебник / В.Л. Матросов. - Москва: Academia, – 2017. – 1040 с.

18 Федотова, Е.Л. Информационные технологии и системы: учебное пособие / Е.Л. Федотова. – Москва: Форум, – 2018. – 149 с.

19 Цветкова, М.С. Информатика и ИКТ: Учебник / М.С. Цветкова. – Москва: Academia, – 2017. – 352 с