МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

«Самарский государственный технический университет»

Институт автоматики и информационных технологий

Кафедра Электронные системы и информационная безопасность

**ЗАДАНИЕ**

**НА ВЫПОЛНЕНИЕ ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ**

СамГТУ 100301.020109.021.01 ТЗ

Обучающемуся\_\_\_\_\_**Чамзинской Дарье Олеговне\_4-АИТ-2\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

*(фамилия, имя, отчество, курс, факультет, группа)*

Тема **«Обеспечение безопасности конфиденциальной информации на предприятии»**\_\_\_\_\_

*(полное название темы квалификационной работы, в соответствии с приказом об утверждении тем ВКР)*

Исходные данные (или цель работы) Разработка системы защиты конфиденциальной информации на предприятии ООО «Новый мир»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*(наименование объекта исследования ; производительность или нагрузка, режим работы; вид сырья или материал изделия; требования к продукту, изделию или процессу; особые условия функционирования или эксплуатации объекта в части требований к безопасности эксплуатации, экологической и экономической целесообразности, оптимальным энергозатратам и т.д*.)

Перечень подлежащих исследованию, разработке, проектированию вопросов:

|  |  |
| --- | --- |
| Наименование вопроса | Результаты освоения ОПОП |
| 1. Обеспечение безопасности конфиденциальной информации |  |
| 1. Информационная система ООО «Новый мир» |  |
| 1. Проведения модели злоумышленника предприятия ООО «Новый мир» |  |
| 1. Разработка и настройка комплекса мер по защите конфиденциальной информации |  |
| 1. Экономическое обоснование | ОК-2 |
| 1. Охрана труда | ОПК-6 |

Перечень презентационного материала:

1. Ценность конфиденциальной информации и способы защиты ее от утечек
2. Предприятие ООО «Новый мир»
3. Общий алгоритм работы системы
4. Алгоритмы работы блокировки социальных сетей и контроля электронной почты
5. Настройка блокировки социальных сетей и контроля электронной почты
6. Блокирование съемных носителей
7. Экономическое обоснование

Нормоконтролер:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*(должность, ф.и.о. нормоконтролера)*

Дата выдачи задания: «» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_г.

Задание согласовано и принято к исполнению.

**Руководитель Студент**

\_Н.Е. Карпова\_\_\_\_\_\_\_\_\_ Д.О. Чамзинская\_\_

*(И. О. фамилия,) (И. О. фамилия)*

*\_\_\_\_\_ Доцент, к.т.н \_\_\_ \_\_\_*4-ИАИТ-2*\_\_\_\_\_\_\_\_\_\_\_*

*(должность, уч. степень, уч. звание) (факультет, группа)*

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

*(подпись, дата) (подпись, дата)*

Тема утверждена приказом по СамГТУ № \_\_\_1/331\_\_\_ от "29"\_\_апреля 2022\_г.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

«Самарский государственный технический университет»

Институт автоматики и информационных технологий

Кафедра Электронные системы и информационная безопасность

**Календарный план**

выполнения выпускной квалификационной работы

Обучающегося\_\_\_\_**Чамзинской Дарьи Олеговны 4-АИТ-2**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*(фамилия, имя, отчество, курс, факультет, группа)*

Тема **«Обеспечение безопасности конфиденциальной информации на предприятии»**\_\_\_\_\_

*(полное название темы квалификационной работы, в соответствии с приказом об утверждении тематики ВКР)*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № | Этапы выполнения ВКР | Дата (срок)  выполнения | | Отметка  о выполнении |
| план | факт |
| 1 | Разработка структуры ВКР. Проведение литературного обзора | 26.11.21 | 26.11.21 |  |
| 2 | Проведение анализа информационной системы конфиденциальной информации ООО «Новый мир» | 16.01.22 | 16.01.22 |  |
| 3 | Проведение анализа угроз безопасности в информационной системе ООО «Новый мир» | 19.02.22 | 19.02.22 |  |
| 4 | Разработка и настройка комплекса мер по защите конфиденциальной информации | 3.03.22 | 3.03.22 |  |
| 5 | Подготовка рукописи ВКР | 30.05.22 | 30.05.22 |  |
| 6 | Доработка текста ВКР в соответствии с замечаниями научного руководителя | 5.06.22 | 5.06.22 |  |
| 7 | Предварительная защита квалификационной работы на кафедре | 10.06.22 | 10.06.22 |  |

Студент Чамзинская Дарья Олеговна

Руководитель Карпова Надежда Евгеньевна

Заведующий кафедрой Скобелев Петр Олегович

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

«Самарский государственный технический университет»

Институт автоматики и информационных технологий

Кафедра Электронные системы и информационная безопасность

Допустить к защите

Заведующий кафедрой\_\_\_\_Скобелев П.О.

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 20 г.

**Выпускная квалификационная работа**

СамГТУ 100301.043.021.02 ПЗ

Тема:\_«**Обеспечение безопасности конфиденциальной информации на предприятии»**

*(полное название темы квалификационной работы, в соответствии с приказом об утверждении тем ВКР)*

Обучающийся **\_Чамзинская Дарья Олеговна 4-АИТ-2**

*(фамилия, имя, отчество, курс, факультет, группа)*

Руководитель работы: к.т.н доцент Карпова Надежда Евгеньевна

*(должность, подпись, дата, фамилия, инициалы)*

Нормоконтролер: ст. преподаватель Андреева Наталья Викторовна

*(подпись, дата, фамилия, инициалы)*

Консультант Андреева Н.В., ст. преподаватель

Консультант Яговкин Н.Г., д.т.н., профессор

Самара 2022г.

**РЕФЕРАТ**

В данной выпускной квалификационной работе пояснительная записка содержит 57 страниц, 30 иллюстраций, 4 таблицы, 10 источников.   
Графический материал выполнен на 7 листах формата А1.  
Ключевые слова:  
Конфиденциальная информация, комплекс мер по защите, угрозы информации.  
В данной выпускной квалификационной работе рассмотрены вопросы, связанные с разработкой системы по обеспечению безопасности конфиденциально информации на предприятии. Во время выполнения работы была проанализирована статистика угроз конфиденциальной информации.   
В результате выполнения ВКР была разработан комплекс мер по защите конфиденциальной информации. Был произведен выбор мер по защите, а также обоснование оборудования для системы защиты, настроен контроль электронной почты, заблокирован доступ к запрещенным сайтам, заблокированы съемные носители.  
В экономической части данной работы было произведено обоснование внедрения разработанной системы, произведены расчеты затрат на ее разработку, а также проведен расчет экономической эффективности спроектированной системы, для чего производились расчеты ЧДС, ВНД и СВПИ.  
В части безопасности жизнедеятельности рассмотрены вопросы проектирования производственного помещения, рабочего места и выбора оборудования с точки зрения охраны труда.

**Содержание**

[ВВЕДЕНИЕ 7](#_Toc105493737)

[Глава 1. Обзор угроз информационной безопасности. 9](#_Toc105493738)

[Глава 2. Обзор систем обеспечения безопасности конфиденциальной информации. 14](#_Toc105493739)

[2.1. DLP – система. 15](#_Toc105493740)

[2.2. InspectSystem. 16](#_Toc105493741)

[2.3. Yaware.TimeTracker. 17](#_Toc105493742)

[Глава 3. Разработка системы защиты конфиденциальной информации предприятия ООО «Новый мир». 18](#_Toc105493743)

[3.1. Рассмотрение информационной системы предприятия ООО «Новый мир». 18](#_Toc105493744)

[3.2. Структура системы защиты конфиденциальной информации. 22](#_Toc105493745)

[3.3. Описание функционирования защиты. 25](#_Toc105493746)

[3.4. Проектирование комплекса мер по защите. 25](#_Toc105493747)

[3.4.1. Блокирование социальных сетей. 25](#_Toc105493748)

[3.4.2. Контроль электронной почты. 28](#_Toc105493749)

[3.4.3. Блокирование съемных носителей. 35](#_Toc105493750)

[Глава 4. Экономическое обоснование. 40](#_Toc105493751)

[4.1. Маркетинговый анализ. 40](#_Toc105493752)

[Глава 5. Охрана труда. 51](#_Toc105493753)

[5.1. Анализ и проектирование производственной среды. 51](#_Toc105493754)

[5.2. Проектирование рабочего места. 52](#_Toc105493755)

[5.3. Выбор оборудования. 53](#_Toc105493756)

[5.4. Проектирование схемы подключения оборудования. 54](#_Toc105493757)

[Заключение 57](#_Toc105493758)

[Список использованной литературы 58](#_Toc105493759)

## ВВЕДЕНИЕ

Информация представляет собой сведения, которые регламентированы правовыми нормами. Существует два вида информации: сведения, находящиеся в открытом и в ограниченном доступе. Между открытой и конфиденциальной информацией имеются принципиальные различия. Распространение конфиденциальной информации создает угрозу экономической безопасности и наказывается в соответствии с действующим законодательством.

Согласно Федеральному закону Российской Федерации «Об информации, информационных технологиях и о защите информации» № 149-ФЗ, сведения делятся на два вида:

* информация для общего пользования. Вид данных, находящихся в открытом доступе для всех граждан РФ;
* данные с закрытым доступом. Вид сведений, которые ограничены нормативно-правовыми актами РФ и доступны только определенным категориям лиц, которые получают доступ к информации в связи со своими служебными полномочиями.

В широком смысле слова, конфиденциальная информация – это сведения с ограниченным доступом. В узком смысле, конфиденциальная информация имеет особую ценность для лиц, пребывающих на государственной службе или работающих в организации.

Конфиденциальная информация представляет собой определенную тайну, поскольку она доступна только нескольким категориям лиц, имеющим право и доступ на работу с ней. Охрана и правовая защита конфиденциальных данных гарантирована государством и закреплена в Конституции РФ. В основном законе РФ указано, что гражданин, организация и государство, имеют право на тайну.

Основными источниками правового регулирования конфиденциальной информации в РФ являются:

* международные договоры и соглашения;
* конституция РФ;
* федеральные законы;
* законы субъектов;
* локальные акты.

Исходя из всего вышеизложенного защита конфиденциальной информации на предприятии является актуальной задачей.

Основной целью данной выпускной квалификационной работы является обеспечение безопасности конфиденциальной информации на предприятии ООО «Новый мир». Задачи, поставленные в работе:

* рассмотрение угроз информационной безопасности;
* обзор систем обеспечения безопасности конфиденциальной информации;
* разработка мер по защите конфиденциальной информации;
* экономическое обоснование разработанной системы защиты.

## Глава 1. Обзор угроз информационной безопасности.

Угрозы информационной (компьютерной) безопасности — это различные действия, которые могут привести к нарушениям состояния защиты информации. Другими словами, это — потенциально возможные события, процессы или действия, которые могут нанести ущерб информационным и компьютерным системам.[4]

Угрозы ИБ можно разделить на два типа:

* естественные
* искусственные.

К естественным относятся природные явления, которые не зависят от человека, например, ураганы, наводнения, пожары и т.д. Искусственные угрозы зависят непосредственно от человека и могут быть преднамеренными и непреднамеренными. Непреднамеренные угрозы возникают из-за неосторожности, невнимательности и незнания. Примером таких угроз может быть установка программ, не входящих в число необходимых для работы и в дальнейшем нарушающих работу системы, что и приводит к потере информации. Преднамеренные угрозы, в отличие от предыдущих, создаются специально. К ним можно отнести атаки злоумышленников как извне, так и изнутри компании. Результат реализации этого вида угроз — потери денежных средств и интеллектуальной собственности организации. [4]

Классификация угроз информационной безопасности

В зависимости от различных способов классификации все возможные угрозы информационной безопасности можно разделить на следующие основные подгруппы:

* Нежелательный контент.
* Несанкционированный доступ.
* Утечки информации.
* Потеря данных.
* Мошенничество.
* Кибервойны.
* Кибертерроризм.

Нежелательный контент — это не только вредоносный код, потенциально опасные программы и спам (т.е. то, что непосредственно создано для уничтожения или кражи информации), но и сайты, запрещенные законодательством, а также нежелательные ресурсы с информацией, не соответствующей возрасту потребителя. [4]

Несанкционированный доступ — просмотр информации сотрудником, который не имеет разрешения пользоваться ею, путем превышения должностных полномочий. Несанкционированный доступ приводит к утечке информации. В зависимости от того, каковы данные и где они хранятся, утечки могут организовываться разными способами, а именно через атаки на сайты, взлом программ, перехват данных по сети, использование несанкционированных программ. Утечки информации можно разделять на:

* умышленные
* случайные.

Случайные утечки происходят из-за ошибок оборудования, программного обеспечения и персонала. Умышленные, в свою очередь, организовываются преднамеренно с целью получить доступ к данным, нанести ущерб. [4]

Потерю данных можно считать одной из основных угроз информационной безопасности. Нарушение целостности информации может быть вызвано неисправностью оборудования или умышленными действиями людей, будь то сотрудники или злоумышленники. [4]

Не менее опасной угрозой является мошенничество с использованием информационных технологий («фрод»). К мошенничеству можно отнести не только манипуляции с кредитными картами («кардинг») и взлом онлайн-банка, но и внутренний фрод. Целями этих экономических преступлений являются обход законодательства, политики безопасности или нормативных актов, присвоение имущества. [4]

Ежегодно по всему миру возрастает террористическая угроза, постепенно перемещаясь при этом в виртуальное пространство. На сегодняшний день никого не удивляет возможность атак на автоматизированные системы управления технологическими процессами (АСУ ТП) различных предприятий. Но подобные атаки не проводятся без предварительной разведки, для чего применяется кибершпионаж, помогающий собрать необходимые данные. Существует также такое понятие, как «информационная война»; она отличается от обычной войны тем, что в качестве оружия выступает тщательно подготовленная информация. [4]

Источник угроз информационной безопасности

Нарушение режима информационной безопасности может быть вызвано как спланированными операциями злоумышленников, так и неопытностью сотрудников. Пользователь должен иметь хоть какое-то понятие об ИБ, вредоносном программном обеспечении, чтобы своими действиями не нанести ущерб компании и самому себе. Такие инциденты, как потеря или утечка информации, могут также быть обусловлены целенаправленными действиями сотрудников компании, которые заинтересованы в получении прибыли в обмен на ценные данные организации, в которой работают или работали.

Основными источниками угроз являются отдельные злоумышленники («хакеры»), киберпреступные группы и государственные спецслужбы (киберподразделения), которые применяют весь арсенал доступных киберсредств, перечисленных и описанных выше. Чтобы пробиться через защиту и получить доступ к нужной информации, они используют слабые места и ошибки в работе программного обеспечения и веб-приложений, изъяны в конфигурациях сетевых экранов и настройках прав доступа, прибегают к прослушиванию каналов связи и использованию клавиатурных шпионов.

То, чем будет производиться атака, зависит от типа информации, ее расположения, способов доступа к ней и уровня защиты. Если атака будет рассчитана на неопытность жертвы, то возможно, например, использование спам-рассылок.

Оценивать угрозы информационной безопасности необходимо комплексно, при этом методы оценки будут различаться в каждом конкретном случае. Так, чтобы исключить потерю данных из-за неисправности оборудования, нужно использовать качественные комплектующие, проводить регулярное техническое обслуживание, устанавливать стабилизаторы напряжения. Далее следует устанавливать и регулярно обновлять программное обеспечение (ПО). Отдельное внимание нужно уделить защитному ПО, базы которого должны обновляться ежедневно. Обучение сотрудников компании основным понятиям информационной безопасности и принципам работы различных вредоносных программ поможет избежать случайных утечек данных, исключить случайную установку потенциально опасного программного обеспечения на компьютер. Также в качестве меры предосторожности от потери информации следует делать резервные копии. Для того чтобы следить за деятельностью сотрудников на рабочих местах и иметь возможность обнаружить злоумышленника, следует использовать DLP-системы. [4]

Организовать информационную безопасность помогут специализированные программы, разработанные на основе современных технологий:

* защита от нежелательного контента (антивирус, антиспам, веб-фильтры, анти-шпионы);
* сетевые экраны и системы обнаружения вторжений (IPS);
* управление учетными данными (IDM);
* контроль привилегированных пользователей (PUM);
* защита от DDoS;
* защита веб-приложений (WAF);
* анализ исходного кода;
* антифрод;
* защита от таргетированных атак;
* управление событиями безопасности (SIEM);
* системы обнаружения аномального поведения пользователей (UEBA);
* защита АСУ ТП;
* защита от утечек данных (DLP);
* шифрование;
* защита мобильных устройств;
* резервное копирование;
* системы устойчивости.

## Глава 2. Обзор систем обеспечения безопасности конфиденциальной информации.

Для предотвращения утечек конфиденциальной информации на предприятии рассмотрим функционал популярных систем контроля сотрудников, узнаем их преимущества и недостатки.

## 2.1. DLP – система.

DLP (Data Loss Prevention) — это программный продукт для предотвращения утечек конфиденциальных данных в корпоративной сети. Это общее определение и название класса ПО, которое создано для защиты данных от несанкционированного доступа.

DLP-система позволяет контролировать каналы передачи данных, выявлять и предотвращать утечки критичной информации. Дает возможность гибко классифицировать данные внутри компании и контролировать их потоки. Также дает возможность искать данные в файловых хранилищах, рабочих компьютерах сотрудников, базах данных и т. д.

Преимущества DLP:

Стандартные меры безопасности включают брандмауэр, систему обнаружения вторжений и антивирусное программное обеспечение. Это механизмы, которые защищают компьютеры от внутренних и внешних атак.

Добавление решения DLP в вашу систему кибербезопасности дает вам следующие преимущества:

* Эффективность для предотвращения внутренних и внешних угроз
* Обеспечение видимости обмена данными
* Применение процедур авторизации перед доступом к конфиденциальным данным
* Применение машинного обучения для выявления ненормального поведения пользователя и маркировки конфиденциальных данных.[8]

Недостатки DLP:

* Высокая стоимость. Бесплатных и open source DLP систем не существует. Это серьезное ПО для решения корпоративных задач, требующее такого же серьезного технического сопровождения. Теоретически бесплатным может быть только совершенно сырой продукт, который в конечном счете станет платным
* Сложный функционал: чтобы установить и правильно настроить требуются опытные специалисты
* Отсутствие гибкости — много возможностей, которые не пригодятся, но заплатить за них придётся
* Требуется закупка оборудования в каждый офис и сопровождение программного обеспечения.[8]

Если рассматривать альтернативы в плоскости контроля выполняемой работы, следует выделить такие элементы:

* Учет дисциплины, расходуемого времени
* Контроль работы в сети интернет
* Контроль работы с клиентами, переписка в мессенджерах и почте
* Возможность проверки выполняемой работы
* Сохранение данных о проделанной работе
* Оповещения о нарушениях

Далее мы будем рассматривать программы, которые будут частично удовлетворять выше перечисленные условия.

## 2.2. InspectSystem.

InspectSystem вместо DLP, является разумным выбором. InspectSystem постоянно контролирует все действия в сети вашей компании, в том числе внутренних и сторонних пользователей. Система также предоставляет вам надежную функцию реагирования на инциденты, которая включает в себя предупреждения и уведомления. InspectSystem в сочетании с простой схемой развертывания является более эффективной и простой в использовании, чем традиционная система DLP.[8]

Основные функции InspectSystem:

* контроль компьютеров каждого подключенного члена команды;
* возможность работы с фрилансерами;
* подсчет времени, потраченного на выполнение обязанностей;
* просмотр диалогов в мессенджерах;
* выявление использования веб-сайтов и приложений, не имеющих отношения к решению поставленных задач;
* получение отчетов о нарушении правил внутреннего распорядка и трудового законодательства;
* настройка параметров оповещения.

Недостатки InspectSystem:

* Подписка покупается отдельно на каждое подключенное устройство
* Система не анализирует полезность действий сотрудника
* Не контролируются действия с переносом данных на другие носители.

## 2.3. [Yaware.TimeTracker](https://startpack.ru/application/yaware-time-tracking).

Yaware.TimeTracker — это сервис, который способен повысить эффективность работников уже в первые недели использования. К тому же, за результатами работы можно следить руководителю с мобильного телефона. к. Система создана с максимальным упором под руководителей: сервис предлагает проводить разного рода анализы выполняемой работы и выставлять оценку персоналу, фиксировать и контролировать сотрудников, которые расходуют время впустую, удерживать дисциплину и оценивать эффективность работы компании в целом.

Благодаря возможностям Yaware вы сможете проконтролировать:

* Присутствие сотрудников на рабочем месте.
* Общий процент отработанного времени и часы сверх нормы.
* Запуск программ и сайтов, которые используют работник.
* Создание снимков экрана и веб-камеры.
* Время работы не за ПК (встречи, переговоры и др.)

Кроме этого, сервис следит за использованием каких-либо ресурсов, выдаёт отчёты в любое время, умеет проводить сравнительный анализ, помогать контролировать сотруднику своё время. Естественно, Yaware.Onlinе пользуется спросом у крупных компаний (логистика, издательства, IT, розничные сети), но и небольшие также часто применяют подобные системы.

Недостатки Yaware.TimeTracker:

* Неудобный интерфейс
* Не контролируются действия с переносом данных на другие носители
* Нет контроля над конфиденциальной информацией
* Подписка покупается отдельно на каждое подключенное устройство.

## Глава 3. Разработка системы защиты конфиденциальной информации предприятия ООО «Новый мир».

## 3.1. Рассмотрение информационной системы предприятия ООО «Новый мир».

Прежде чем начать проектирование системы защиты рассмотрим информационную систему предприятия.

Небольшая компания ООО «Новый мир» занимается продажей деталей для автомобилей. Компания расположена в кирпичном одноэтажном здании, две стороны которого выходят во внутренний двор, где расположены жилые четырех и двухэтажные дома, а две остальные стороны здания выходят на проезжую часть, где расположен автосалон. С противоположных сторон от дороги расположены ТРК и жилой дом. Теплотрасса расположена под проезжей частью.

В компании работает 20 человек: 10 человек занимаются работой с клиентами (составление договоров о продаже; поиск деталей по заказу, поиск клиентов и т.п.), 2 уборщицы, 2 сотрудника отдела информационной безопасности, 2 охранника, секретарь (работает с директором компании), бухгалтер, заместитель директора, директор.

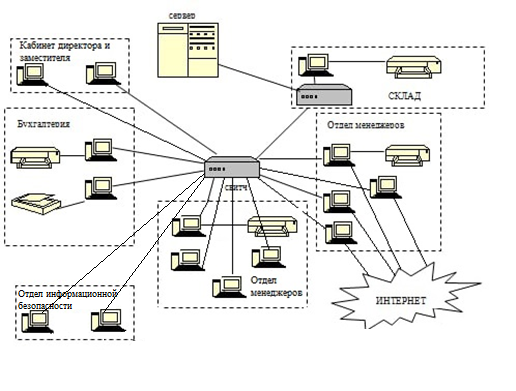


Рисунок 3.1.1 – Информационная система предприятия.

Компания работает под управлением операционной системы Windows 10. Для выполнения должностных обязанностей установлено следующее программное обеспечение:

* Пакет Microsoft Office.

Учетная запись пользователя имеет доступ в сеть Интернет и в локальную сеть предприятия, в которой расположен общий ресурс для хранения документов.

Ценность на данном предприятии представляет клиентская база, договоры купле продажи деталей автомобилей.

По данным InfoWatch (российский разработчик решений для обеспечения информационной безопасности организаций) главную угрозой для фирмы является внутренний нарушитель.

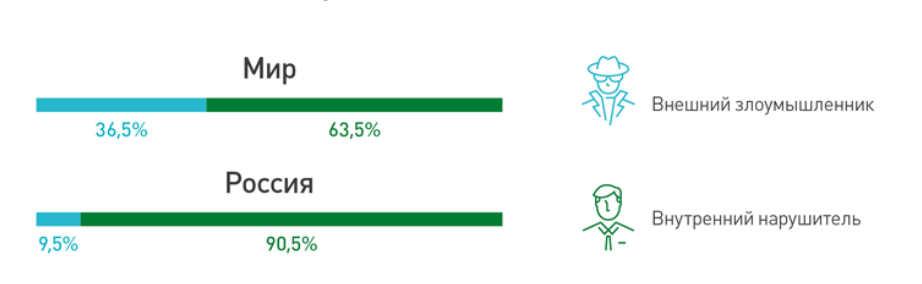


Рисунок 3.1.2 – Распределение утечек конфиденциальной информации по вектору воздействия, мир – Россия, 2018.

А именно сотрудник, работающий на данный момент в компании.

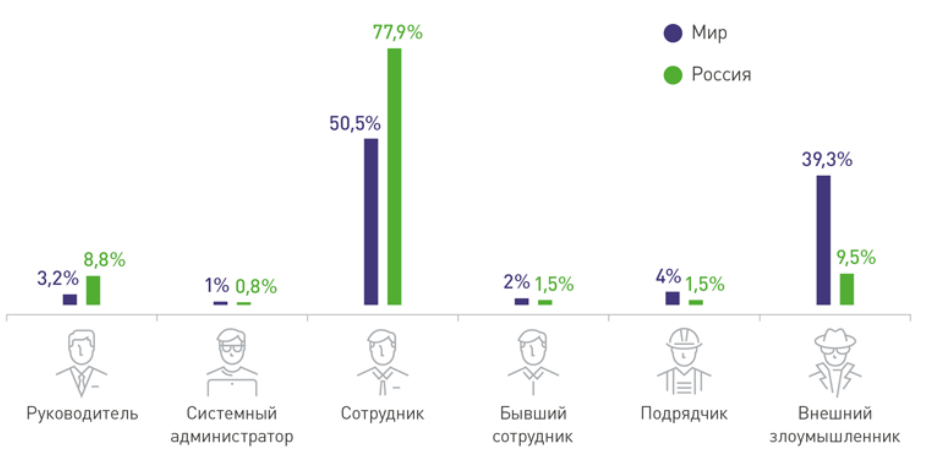


Рисунок 3.1.3 – Распределение утечек конфиденциальной информации по виновнику, мир – Россия, 2018.

Далее с помощью статистики определим, какие каналы утечки стоит в первую очередь обезопасить.



Рисунок 3.1.4 – Распределение утечек конфиденциальной информации по каналам, мир – Россия, 2018.

Из вышеприведенного рисунка видно, что сотрудники могут передать информацию с помощью таких каналов, как съемные носители, сеть (социальные сети) и электронная почта.

Чтобы защитить данное предприятие далее мы будем разрабатывать свою систему защиты, которая предотвратит утечку конфиденциальной информации.

## 3.2. Структура системы защиты конфиденциальной информации.

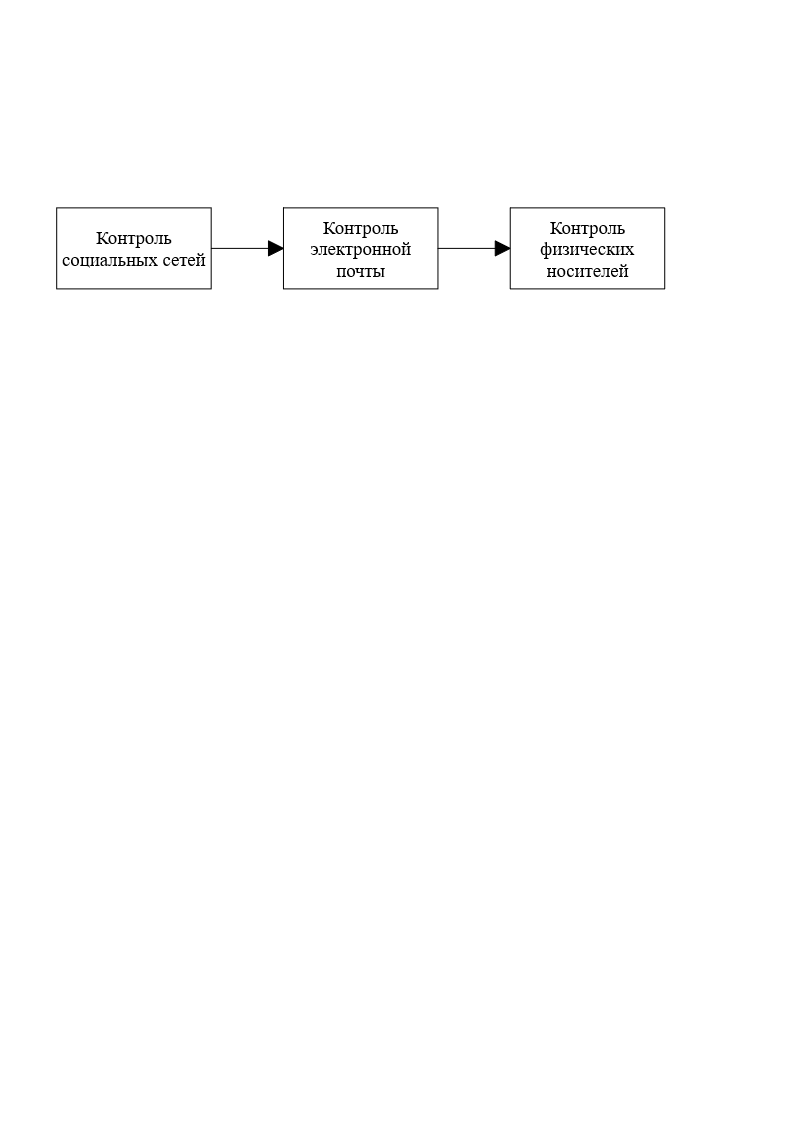
****

Рисунок 3.2.1 – Структура система защиты, которая будет реализована.

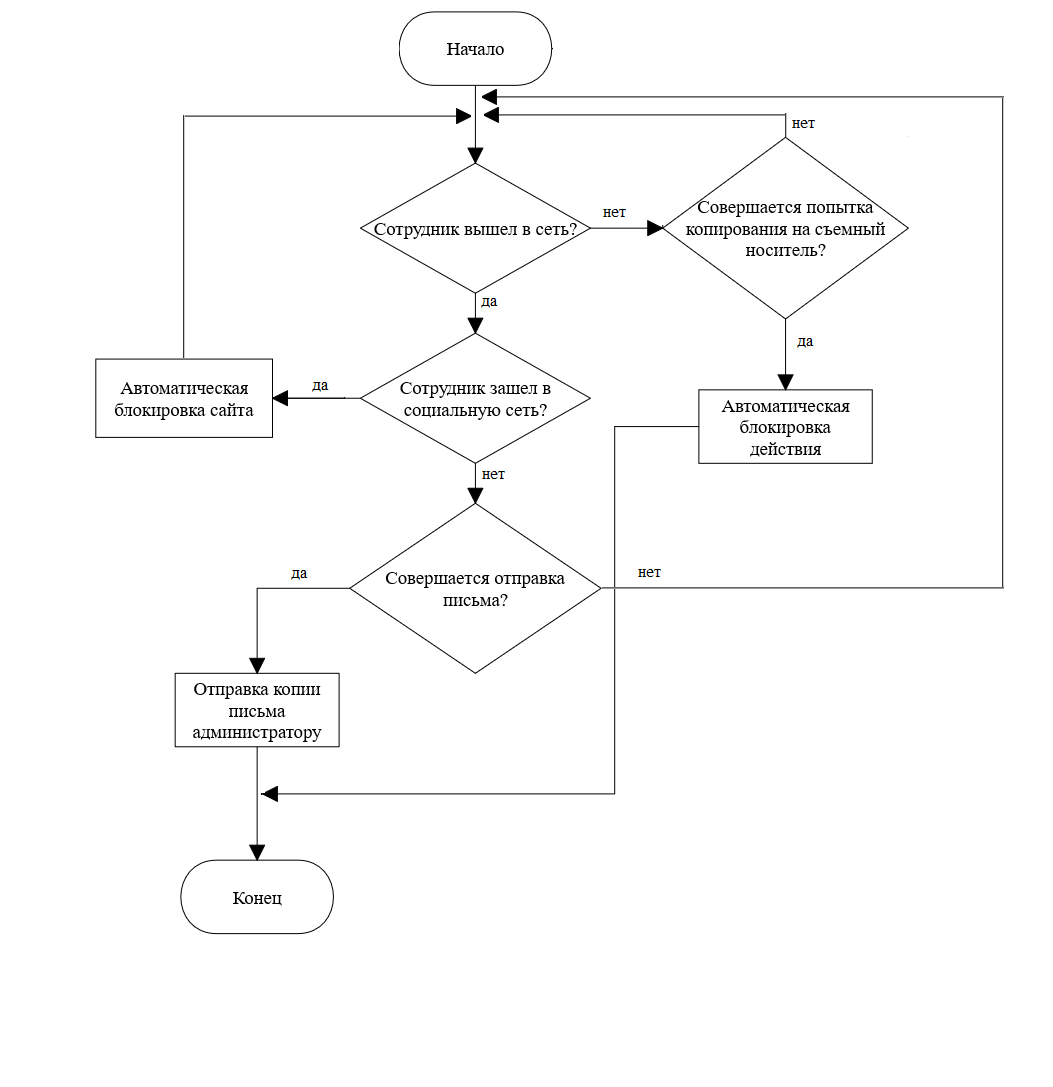
****

Рисунок 3.2.2 – Общий алгоритм работы комплекса мер по защите.

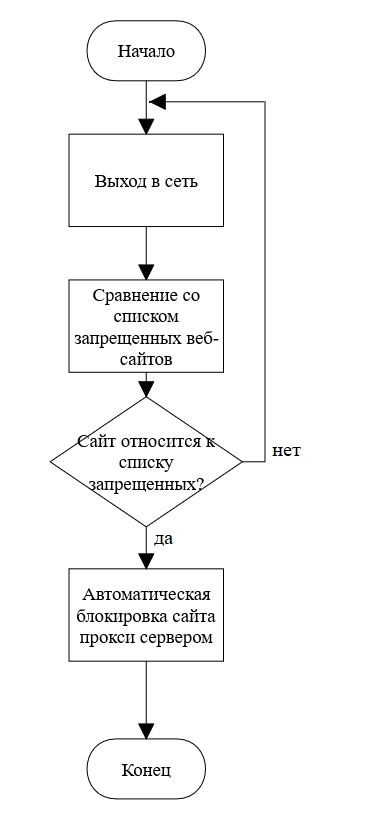
****

Рисунок 3.2.3 – Алгоритм работы системы контроля социальных сетей.

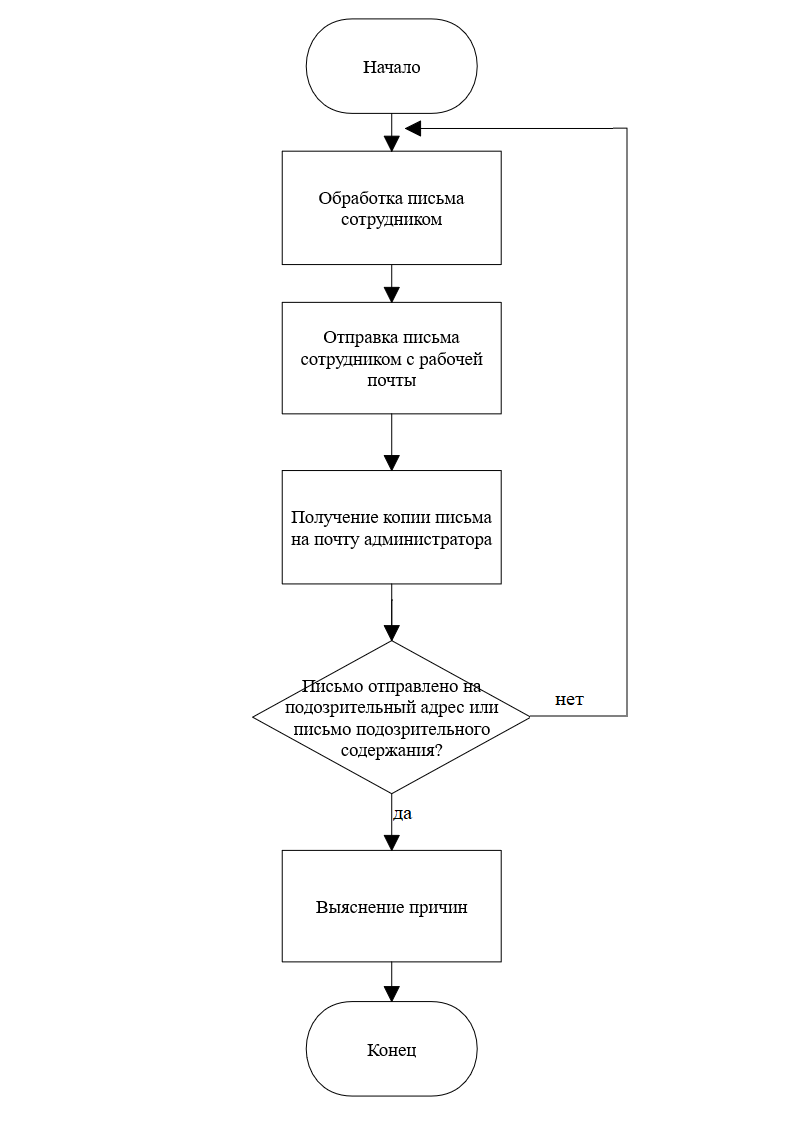
****

Рисунок 3.2.4 – Алгоритм работы системы контроля электронной почты.

## 3.3. Описание функционирования защиты.

Чтобы обеспечить безопасность конфиденциальной информации от пересылок через социальные сети и почту, мы будем использовать бесплатную операционную систему Ubuntu.

Для осуществления защиты информации от копирования с помощью социальных сетей, мы установим бесплатный программный пакет Squid, который реализует функцию кэширующего прокси-сервера для протоколов HTTP, FTP, Gopher и (в случае соответствующих настроек) HTTPS. Разработан он сообществом как программа с открытым исходным кодом (распространяется в соответствии с GNU GPL). Все запросы выполняет как один неблокируемый процесс ввода-вывода.

Далее нам необходимо осуществить контроль электронной почты сотрудников фирмы. Мы установим бесплатный программный пакет Postfix, после настройки которого мы сможем получать на почту администратора копии всех писем с рабочих электронных почт. В случае подозрительного сообщения или адреса отправки сообщения, сотрудника вызывают для выяснения причин.

Для того чтобы сотрудники не могли копировать, читать и переносить какую-либо постороннюю информацию на рабочий компьютер, воспользуемся помощью редактора локальной групповой политики.

## 3.4. Проектирование комплекса мер по защите.

## 3.4.1. Блокирование социальных сетей.

Так как для небольшой компании внедрении DLP-системы слишком затратно, то попробуем собрать из вспомогательных программных пакетов свою защищенную систему.

Для этого была установлена виртуальная машина, и был установлен дистрибутив Ubuntu версии 20.04.3 LTS.

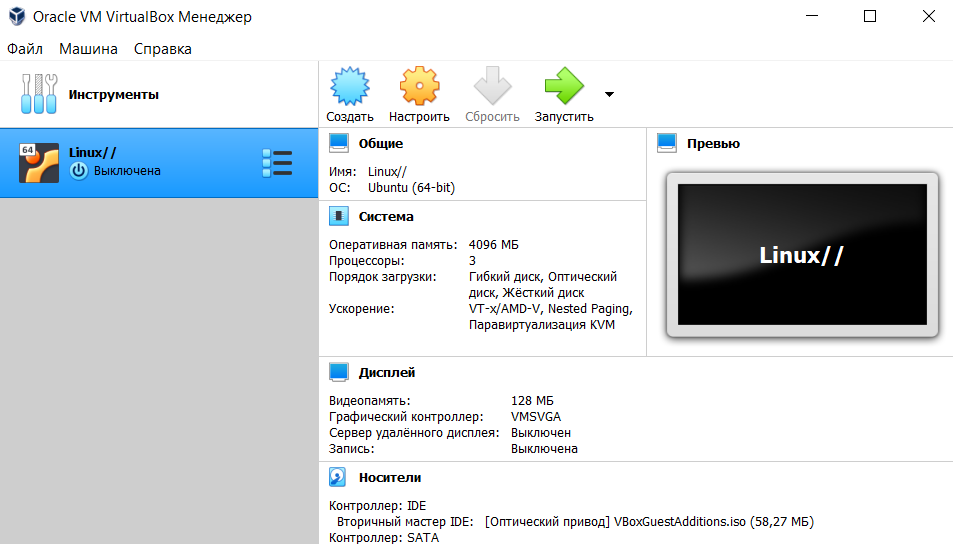


Рисунок 3.4.1 – виртуальная машина в Oracle VirtualBox.

Пакет Squid доступен в стандартном репозитории. Для установки выполним команду:

$ sudo apt-get -y install squid

Запустим Squid и зададим запуск при загрузке:

$ sudo systemctl start squid

$ sudo systemctl enable squid

После этого можем проверить статус службы следующей командой:

$ sudo systemctl status squid

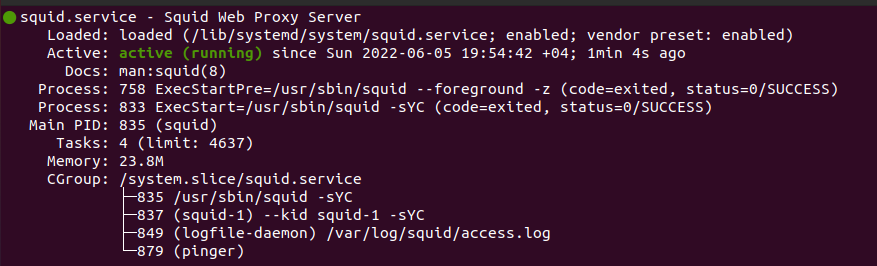


Рисунок 3.4.2 – Статус службы Squid.

Важные файлы Squid располагаются в следующих директориях:

Файл конфигурации: /etc/squid/squid.conf  
Журнал доступа: /var/log/squid/access.log  
Журнал кэша: /var/log/squid/cache.log

Для блокировки доступа к нежелательным веб-сайтам сначала создайте файл с “черным списком”:

$ sudo touch /etc/squid/blacklisted\_sites.acl

Теперь в данный файл нужно добавить сайты, к которым требуется заблокировать доступ. Заблокируем доступа к одноклассникам, вконтакте и яндекс дзен:

.vk.com

.ok.ru

.zen.yandex.ru

Точки перед именами указывают Squid блокировать все ссылки на эти сайты, в том числе www. vk.com, subsite.vk.com и т.д.

Далее нужно открыть файл конфигурации

$ sudo vim /etc/squid/squid.conf

Добавим список контроля доступа по доменным именам, указанным в файле, а также правило, запрещающее доступ для этого списка:

acl bad\_urls dstdomain "/etc/squid/blacklisted\_sites.acl"

http\_access deny bad\_urls

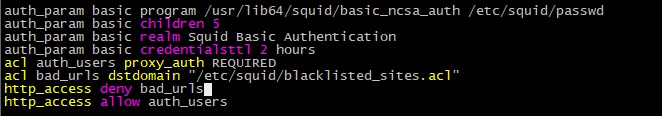
[](https://itproffi.ru/wp-content/uploads/2019/02/squid4.jpg)

Рисунок 3.4.3 – Добавление списка контроля доступом и правило, запрещающее доступ для списка.

Сохраним файл и перезапустим Squid:

$ sudo systemctl restart squid

Установив пакет Squid, настроив его, создаем файл, в котором прописали сайты, для которых запрещен доступ.

Попробуем теперь зайти на один из сайтов и видим, что при попытке зайти в социальную сеть получаем такую картинку:

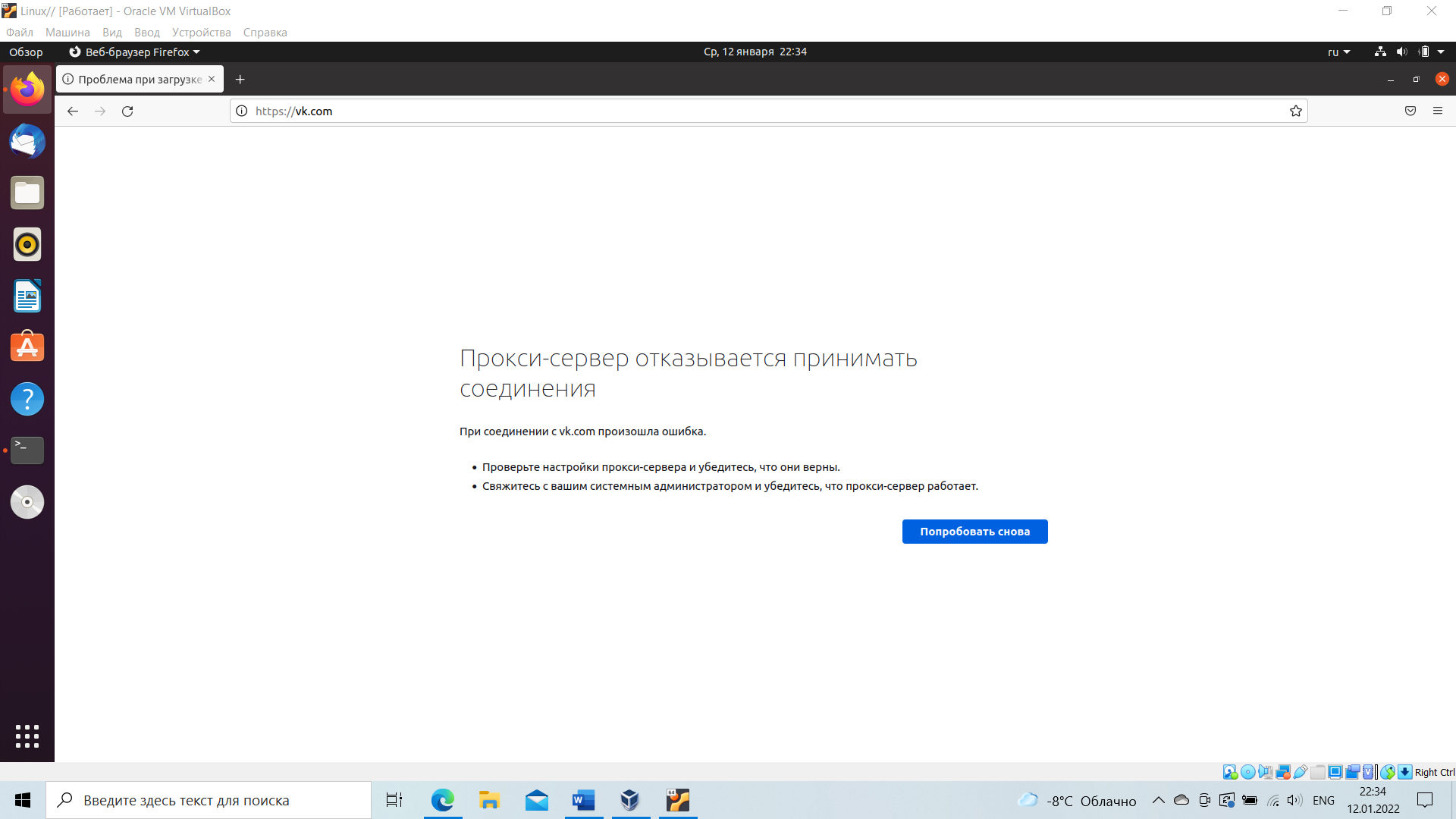


Рисунок 3.4.4 - Попытка зайти на сайт «Вконтакте» после настройки Squid.

Данная функция поможет нам предотвратить утечку через соцсети. Также можно настроить и другие сайты, на которые доступ работникам будет запрещен для предотвращения каких-либо утечек.

## 3.4.2. Контроль электронной почты.

Для контроля электронной почты сотрудников установим пакет Postfix.

Для начала обновим локальный кэш пакетов apt, для этого мы открываем командную строку и вводим следующую команду:

~$ sudo apt update

Далее устанавливаем сам Postfix с помощью команды:

~$ sudo apt-get install postfix

При конфигурировании пакета нам задаются несколько вопросов, внимание стоит обратить лишь на предлагаемые профили первоначальной настройки. Вне зависимости от того, для чего мы хотим использовать Postfix, всегда выбираем Internet Site. Это необходимо для того, чтобы Postfix сгенерировал нам файл main.cf и сразу приступил к работе. В противном случае нам бы пришлось конфигурировать этот файл самостоятельно.

Приведем настройки, которые я использовала:

* General type of mail configuration?: Internet Site
* System mail name: example.com (не mail.example.com)
* Root and postmaster mail recipient: имя пользователя основной учетной записи Linux (в наших примерах sammy)
* Other destinations to accept mail for: $myhostname, example.com, mail.example.com, localhost.example.com, localhost
* Force synchronous updates on mail queue?: No
* Local networks: 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
* Mailbox size limit: 0
* Local address extension character: +
* Internet protocols to use: all

Примечание. Если впоследствии нам понадобится изменить эти настройки, будем вводить команду:

~$ dpkg-reconfigure postfix

Для параметров будут указаны заданные ранее значения.

Отправка почты из Postfix через Gmail.

Настройка аутентификации в Gmail

Создам файл паролей, который будет использовать Postfix для аутентификации в Gmail. Заменим имя пользователя своим именем пользователя и паролем Gmail на свой пароль Gmail.

Файл пароля будет находиться в каталоге конфигурации Postfix и называется sasl\_passwd.

Конфигурационные файлы Postfix находятся в каталоге /etc/postfix. Отредактируем файл паролей:

~$ sudo nano /etc/postfix/sasl\_passwd

Добавим строку:

Изображение выглядит как текст, монитор, компьютер, экран

Автоматически созданное описание

Рисунок 3.4.5 - Настройка почты администратора.

Сохраняем и закрываем файл. Наш пароль Gmail хранится в виде открытого текста, поэтому файл должен быть доступен только пользователю root. Для этого выполняем команду:

~$ sudo chmod 600 /etc/postfix/sasl\_passwd

Настройка Postfix

В файле конфигурации Postfix main.cf присутствуют шесть параметров, которые должны быть установлены:

**1. relayhost** – указывает почтовый хост и номер порта. Имя хоста будет заключено в квадратные скобки, чтобы указать, что поиск MX не требуется.

**2. smtp\_use\_tls** – включает (или отключает) безопасность транспортного уровня.

**3. smtp\_sasl\_auth\_enable** – включает (или отключает) аутентификацию SASL.

**4. smtp\_sasl\_security\_options** – в нашей конфигурации будет установлен пустым, чтобы гарантировать, что никакие параметры безопасности, несовместимые с Gmail, не используются.

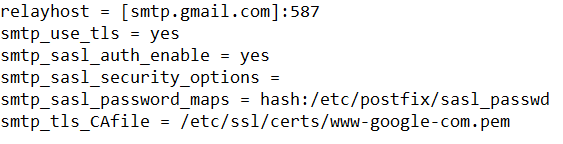
**5. smtp\_sasl\_password\_maps** – указывает на файл паролей. Этот файл будет скомпилирован и хеширован postmap на следующем шаге.

**6. smtp\_tls\_CAfile** – указывает список центров сертификации, которые будут использоваться при проверке подлинности сервера.

Отредактируем основной файл конфигурации Postfix:

~$ sudo nano /etc/postfix/main.cf

Добавим следующие значения:

**,**

где www-google-com.pemэто файл, содержащий сертификат google.com.

Сохраним и закроем main.cf.

Обработка файла паролей

Используем postmap для компиляции и хэширования содержимого sasl\_passwd. Результаты будут сохранены в нашем каталоге конфигурации Postfix в файле sasl\_passwd.db:

~$ sudo postmap /etc/postfix/sasl\_passwd

Перезапустим Postfix, чтобы изменения вступили в силу.

~$ sudo systemctl restart postfix.service

Включим «разрешить небезопасным приложениям доступ к аккаунту» в Gmail

Откроем страницу Аккаунт Google.

На панели навигации слева выбираем «Безопасность».  
В разделе «Ненадежные приложения», у которых есть доступ к аккаунту в нижней части, страницы нажимаем «Открыть доступ».

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 3.4.6 - Настройка аккаунта Google.

Отправка тестового письма.

Проверим нашу новую конфигурацию, отправив электронное письмо с помощью команды mail. В командной строке выполним:

~$ mail -s "Test " lubasss048@gmail.com,

где lubasss048@gmail.com - электронная почта, на которую отправляется письмо.

Нам будет представлена ​​пустая строка (или поле CC:, которое мы можем пропустить, нажав Enter). Введем текст нашего сообщения, нажимая Enter для перехода на новую строку. Когда закончим составлять письмо, нажимаем CTRL-D, чтобы отправить его.

Изображение выглядит как текст, монитор, снимок экрана, электроника

Автоматически созданное описание

Рисунок 3.4.7 - Тестовое сообщение.

На данную почту пришло наше тестовое сообщение:

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 3.4.8 - Проверка наличия тестового сообщения на почте администратора.

Далее смоделируем так, что все отправляемые нами письма на внешнюю почту приходили копии на mariya56467@gmail.com.

Для этого заходим в файл /etc/postfix/main.cfи добавляем строку, в которой указываем почту, на которую будут приходить копии сообщений.

Изображение выглядит как текст, монитор, снимок экрана, ноутбук

Автоматически созданное описание

Рисунок 3.4.9 - Настройка отправки копий сообщений на почту администратора.

Перезапускаем Postfix c помощью команды:

**~$ sudo systemctl restart postfix**

Далее пробуем также отправить сообщение на почту lubasss048@gmail:

Изображение выглядит как текст, монитор, снимок экрана, экран

Автоматически созданное описание

Рисунок 3.4.10 - Написание тестового сообщения.

Проверим пришли ли сообщения на почту lubasss048@gmail:

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 3.4.11 - Проверка наличия письма на почте сотрудника отдела продаж.

После этого мы должны проверить пришла ли копия сообщения на нашу почту mariya56467@gmail.com. Получили скрытую копию:

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 3.4.12 - Проверка наличия копии отправленного письма на почте администратора.

## 3.4.3. Блокирование съемных носителей.

Для того чтобы сотрудники не могли копировать, читать и переносить какую-либо постороннюю информацию на рабочий компьютер, воспользуемся помощью редактора локальной групповой политики.

Для этого мы нажмем клавиши Win+R на клавиатуре, введите gpedit.msc и нажмите Enter, откроется редактор локальной групповой политики.

Далее нам требуется запретить использование USB накопителей для всех пользователей компьютера, переходим к разделу Конфигурация компьютера — Административные шаблоны — Система — Доступ к съемным запоминающим устройствам.

Нужно обратить внимание на пункты «Съемные диски: «Запретить выполнение», «Съемные диски: Запретить запись», «Съемные диски: Запретить чтение». Все они отвечают за блокировку доступа к USB-накопителям. При этом запрет чтения запрещает не только просмотр содержимого флешки или копирование с неё, но и остальные операции (на накопитель нельзя будет что-либо записать, запуск программ с него также не будет выполняться).

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 3.4.13 - Редактор локальной групповой политики.

Включаем данные политики:

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 3.4.14 - Включение запрета на запись, чтение, выполнение со съемных дисков.

Пробуем подключить USB-носителя после установки политик и получаем следующее:

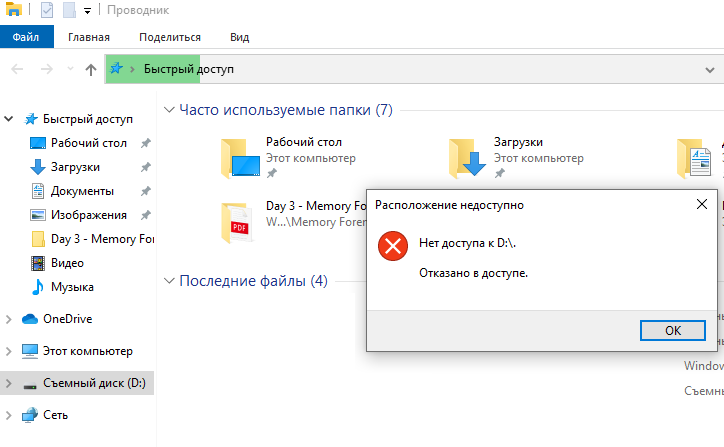


Рисунок 3.4.15 - Проверка при включении USB-носителя.

Сейчас многие компьютеры имеют разъем USB Type-C, через который можно подключить телефон и также совершать различные действия с информацией. Для того, чтобы обезопасить нашу информацию и от этого снова зайдем в редактор локальной групповой политики и включаем «Съемные запоминающие устройства всех классов: Запретить любой доступ».

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 3.4.16 - Включение политики запрета на запоминающие устройства всех классов.

Проверим работоспособность, подключив телефон:

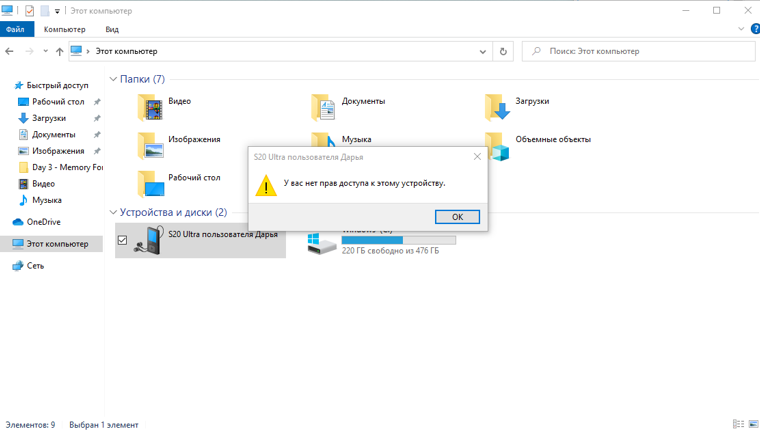


Рисунок 3.4.17 - Подключение телефона через разъем USB Type-C.

Также я пробовала подключить внешний дисковод через USB разъем:

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 3.4.18 - Подключение CD-дисковода.

Таким образом, благодаря редактору групповых политик мы можем остановить копирование, чтение, замену или добавление информации с помощью физических носителей.

## Глава 4. Экономическое обоснование.

## 4.1. Маркетинговый анализ.

В данной выпускной квалификационной работе разрабатывается комплекс мер по защите конфиденциальной информации с помощью контроля электронной почты и блокировки социальных сетей. Это позволяет с наименьшей задержкой реагировать на различные инциденты в информационной системе предприятия, что в свою очередь может уберечь от утечки или уничтожении конфиденциальной информации, следовательно, уберечь от крупного ущерба.

Таким образом можем сделать вывод, что разрабатываемая система может уберечь от возможного нанесения ущерба, а также она снизит нагрузку на персонал, при том, что затраты на такую систему минимальны.

Для оценки конкурентоспособности товара, прежде всего надо выявить, какая продукция является реально или потенциально конкурирующей. Предварительно разрабатывается таблица 8, в которых отражаются значения исследуемых параметров товаров.

Таблица 8 – Система контроля сотрудников

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Наименование конкурирующего товара** | **Авторизация пользователей** | **Предоставление информации** | **Простота использования** | **Дороговизна** |
| комплекс мер по защите конфиденциальной информации с помощью контроля электронной почты и блокировки социальных сетей | Нет | Да | Да | Нет |
| DLP-система | Да | Да | Нет | Да |

Анализ конкурентоспособности товара выполняется на основе таблицы 9, отражающих рейтинг конкурентоспособности, в которых указаны балльные оценки параметров товаров.

Таблица 9 – Система контроля сотрудников

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Наименование конкурирующего товара** | **Характеристики конкурирующего товара** | | | |
| **Авторизация пользователей** | **Предоставление информации** | **Простота использования** | **Дороговизна** |
| **2** | **2** | **2** | **3** |
| Комплекс мер по защите конфиденциальной информации с помощью контроля электронной почты и блокировки социальных сетей | 0 | 3 | 4 | 2 |
| DLP-система | 1 | 3 | 1 | 0 |

Далее необходимо рассчитать интегральный показатель конкурентоспособности для каждого продукта. Величины интегральных показателей выбранных продуктов приведены в таблице 10.

Таблица 10 - Интегральные показатели продуктов

|  |  |
| --- | --- |
| **Наименование товара** | **Интегральный показатель**  **конкурентоспособности** |
| **Система контроля сотрудников** | |
| Комплекс мер по защите конфиденциальной информации с помощью контроля электронной почты и блокировки социальных сетей | 20 |
| DLP-система | 10 |

4.2. Расчеты затрат на создание продукта

4.2.1. Расходы по зарплате исполнителям.

(4.1)

- основная зарплата работников, определяемая в зависимости от трудоемкости этапов разработки, квалификации и уровня оплаты.

(4.2)

m – количество этапов разработки;

n – количество разработчиков, принимающих участие в процессе разработки;

– часовая зарплата разработчика;

– затраты времени в часах i-го разработчика на j-ом этапе;

m=3

n=1

=500руб/час

=16 часов

Все виды работ выполняются 1 человеком, в которые входят 3 этапа проектирования.

1. Разработка технического задания;
2. Настройка работы системы;
3. Сдача продукции заказчику.

Коэффициенты, учитывающие дополнительную заработную плату и отчисления в социальные фонды:

=0,08

=0,3

Получаем следующие значения:

р.

р.

5.2.2. Расходы по арендной плате за помещение.

Проектирование, разработка осуществляется в офисном помещении площадью 11 м².

Расчет затрат на арендную плату вычисляется по следующей формуле:

(4.3)

– арендная плата за 1 м² площади в год

– арендуемая площадь кв.м

– время на разработку в календарных днях

=7000р/м²

=11 м²

=2 дня

Помещение арендуется на две недели, его стоимость составит:

р.

5.2.3. Размер необходимой арендуемой площади.

(5.4)

– 6 м² (норма площади на 1 человека)

Так как в работе над проектом будет задействован 1 человек, необходимая площадь составит 6 м².

Площадь арендованного помещения составляет м², что соответствует требованиям.

5.2.4. Расходы на освещение и отопление

(4.5)

Суммарная мощность энергоприемников 0,52 кВт.

tдн=16 часов;

Тразр.раб=2 дня;

Wэ=4,46 р за 1кВт/ч;

Wтепл=420 р за 1 м2.

Зэн=0,52\*16\*2\*4,46+(11\*2/365)\*420=74,3 р.

5.2.5. Расходы на оплату машинного времени

(4.6)

Стоимость одного машино-часа составляет 160 р.

Рассчитаем оплату машинного времени при продолжительности 3 этапов по 3 часа каждого: Змаш=160\*9=1440 р.

5.2.6. Косвенные расходы организации разработчика

(4.7)

Ккосв=1,3

Зкосв=24000\*1,3=31200 р.

Делаем вывод, что затраты на проектирование составляют:

33696+421,9+74,3+1440+31200=66832,2 р.

4.3. Затраты на изготовление проектируемого чат-бота

Для разработки необходимым является наличие ноутбука стоимостью 50500 р.

Таблица 1. Затраты на изготовление проектируемого изделия

|  |  |  |  |
| --- | --- | --- | --- |
| № | Наименование статей калькуляции | Затраты | |
| руб | % |
| 1 | Покупные изделия и полуфабрикаты | 50500 | 86,32 |
| 2 | Транспортные заготовительные расходы | 2020 | 3,45 |
| Итого основных материалов и покупных изделий | | 52520 р | |
| 3 | Тарифная зарплата производственных рабочих | 1500 | 2,56 |
| 4 | Премия производственных рабочих | 500 | 0,85 |
| Итого зарплата производственных рабочих | | 2000 р | |
| 5 | Дополнительная зарплата производственных рабочих | 550 | 0,94 |
| 6 | Отчисления в социальные фонды | 663 | 1,13 |
| 7 | Внепроизводственные расходы | 2766 | 4,72 |
| Итого производственная себестоимость | | 58499 | 100 |

Стоимость проектирования, внедрения разработки составляет:

И=66832,2 +58499= 125 331,2 р.

4.4. Расчет экономической эффективности проекта

Цель данного раздела – определение показателей экономической эффективности затрат на приобретение новых аппаратных средств защиты информации, средств автоматизации и регулирования производственных процессов. Эти затраты для пользователя носят характер инвестиций.

Поскольку инвестирование - это долговременный процесс, для определения экономической эффективности инвестиций используются методы, основанные на дисконтированных оценках.

Необходимо провести обоснование пороговой процентной ставки (r), на основании которой рассчитываются коэффициенты дисконтирования К:

(4.8)

r=25%; t=5.

K1=0,8 K2=0,64 K3=0,512 K4=0,4096 K5=0,32768

5.4.1. Затраты на текущий ремонт и межремонтное обслуживание

(4.9)

Sэл – стоимость заменяемых в процессе ремонта элементов

Зр – зарплата ремонтных рабочих

(4.10)

Тгод – годовой фонд времени работы проектируемого объекта

Si – стоимость 1 шт i–го элемента

ni – количество элементов каждого i–го наименования

λi – интенсивность отказов i–го элемента, 1/ч

i – число наименований элементов в схеме

(4.11)

Кс – коэффициент, учитывающий премию, дополнительную зарплату и отчисления в социальные фонды

tp – среднее время в часах, затрачиваемое на устранение одного заказа на ремонт или замену невосстанавливаемых элементов

rcp – средняя зарплата ремонтных рабочих.

Затраты на ремонт составляют:

Рт=3165,57+1236,84=4 402,41 р.

4.4.2. Амортизационные отчисления

(4.12)

При норме амортизационных отчислений 15% и первоначальной стоимости техники и работы в рублях составит А=58499\*15/100=8774,85 р.

4.4.3. Эксплуатационные расходы

(4.13)

Э=2600+4402,41+1657+8774,85=17434,26р.

5.4.4. Расчет дисконтированной стоимости

Чистая дисконтированная стоимость рассчитывается по следующей формуле:

(4.14)

(4.15)

(4.16)

Эс=75500 р/год (дополнительные расходы на постоянный мониторинг за состоянием системы).

Эн=17434 р/год

∆Эi=75500 - 17434=58 066 р.

ЧДП= 58 066 р.

r=25%

Рассчитаем ЧДС:

ЧДС=(58066\*0,8+58066\*0,64+58066\*0,512+58066\*0,4096+58066\*0,32768) – 125331,2=156156,04 - 125331,2=30824,84 р.

ЧДС>0, следовательно, затраты оправданы.

r1= 36%, ЧДС=1295,557

r2=37%, ЧДС=-913,58

4.4.5. Расчет внутренней нормы доходности

(4.17)

ВНД=0,36+(1295,557\*(0,37-0,36))/( 1295,557+913,58)=0,3658.

0,3658>0,25, ВНД>r, следовательно затраты оправданы.

4.4.6. Расчет срока полного возмещения инвестиций

(4.18)

И=125331,2 р.

СВПИ=2+(125331,2 -83615)/113345=3,2 года.

В результате проделанной работы можно сделать следующий вывод: при ставке 25% ЧДС составит 30824,84, что говорит об экономической эффективности проекта, а ВНД=48%, больше 25%, что свидетельствует об устойчивости проекта. Срок полного возмещения инвестиций составляет 2,3 года.

## Глава 5. Охрана труда.

## 5.1. Анализ и проектирование производственной среды.

Данное помещение находится в офисном здании. Так как это беспыльное, сухое помещение с нормальной температурой воздуха и с изолирующим (деревянным) полом, в котором отсутствуют условия, свойственные помещениям с повышенной опасностью и особо опасным, то по степени поражения людей электрическим током относится к помещениям без повышенной опасности.

По взрывопожароопасности данное помещение относится к категории «В» - пожароопасное (в нем имеются твердые сгораемые вещества в материалы). В связи с этим помещение оснащено двумя ручными углекислотными огнетушителями (ОУ-5). Первый расположен в углу возле двери, другой в противоположном углу около рабочего места сотрудника.

Помимо огнетушителей около рабочего места размещена аптечка. В помещении установлена система контроля климата (сплит система), которая поддерживает в теплое время года комфортную температуру (21-24°С). В холодное время года помещение отапливается радиаторными батареями.

Относительная влажность воздуха находится на уровне 40-60% и скорость движения не более 0,1м/с.

Офисное здание находится недалеко от оживленной улицы, следовательно, к вопросу шумоизоляции должен быть серьезный подход. Уровень шума не превышает 25-35дБА. Так как помещение оборудовано шумозащитным окном с 5-камерной профильной системой и толщиной внешней стенки 3 мм, дополненным ассиметричным двухкамерным стеклопакетом 32 мм.

В помещении имеются источники искусственного и естественного освещения. На поверхности стола освещенность находится на уровне 400лк. Освещение установлено так. Что не создает бликов на поверхности экрана. Освещенность поверхности экрана составляет 2700лк. Коэффициент естественной освещенности составляет 1,6%.

## 5.2. Проектирование рабочего места.

В данном помещении площадью 11 м² размещается одно рабочее место (рисунок 1). Оно оборудовано жидкокристаллическим монитором (необходимая площадь на одно рабочее место – 4,5 м²), поэтому такой площади для одного человека вполне достаточно.

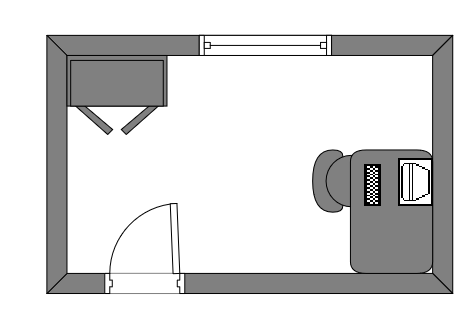


Рисунок 5.2.1 – Рабочее место сотрудника отдела информационной безопасности.

Рабочее место по отношению к световому проему расположено так, чтобы естественный свет падал слева.

Конструкция рабочего стула (кресла) обеспечивает поддержание рациональной рабочей позы при работе на ПЭВМ, позволяет изменять позу с целью снижения статического напряжения мышц шейно-плечевой области и спины для предупреждения развития утомления. Рабочий стул (кресло) является подъемно-поворотным с возможностью регулировки по высоте и углам наклона сиденья и спинки, а также расстоянию спинки от переднего края сиденья, при том, что регулировка каждого параметра независимая, легко осуществляемая и имеет надежную фиксацию. Верхний материал сиденья, спинки и других элементов стула (кресла) полумягкий, с нескользящим, слабо электризующимся и воздухопроницаемым покрытием, которое обеспечивает комфортную посадку и легкую очистку от различных загрязнений.

Высота рабочей поверхности равна 725 мм и не имеет возможности для регулировки. Также рабочее место оборудовано подставкой для ног глубиной 550 мм и шириной 450 мм. Экран видеомонитора расположен на расстоянии 600 мм от глаз пользователя, а клавиатура расположена на рабочей поверхности стола на расстоянии 150 мм от обращенного к пользователю края.

Размещение рабочего стола и стула изображено на рисунке 5.2.1.

Подходящий под описанные критерии стул: «Бюрократ CH 279» (Код товара: 1126585)

Подходящий под описанные критерии стол: «Бюджет» (Артикул: 402661-430 640620)

### 5.3. Выбор оборудования.

1. Для работы спроектированной системы защиты необходим сервер с многоядерным процессором и большим объемом оперативной памяти. Для этих целей выбран сервер «HPE ProLiant MicroServer Gen10 Plus» со следующими характеристиками:

Таблица 5.3.1 – Характеристики HPE ProLiant MicroServer Gen10 Plus

|  |  |
| --- | --- |
| Модель процессора | Intel Pentium G5420 |
| Количество ядер | 2 |
| Частота процессора | 3.6 ГГц |
| Объем ОЗУ | 32 Гб |
| Объем жесткого диска | 1 Тб |

1. Выбранный монитор:  «Philips 243V7QJABF». Его характеристики:

Таблица 5.3.2 – Характеристики Philips 243V7QJABF

|  |  |
| --- | --- |
| Диагональ экрана (дюйм) | 23.8 " |
| Максимальное разрешение | 1920×1080 |
| Тип подсветки матрицы | LED |
| Технология изготовления | IPS |
| Соотношение сторон | 16:9 |

1. Необходимость использования дополнительного оборудования отсутствует.
2. Так как данная система отвечает за безопасность конфиденциальной информации на предприятии, она должна быть оснащена бесперебойным питанием, в противном случае, при ее отключении вся система становится уязвимой, что может повлечь за собой серьезный ущерб. В связи с этим используется источник бесперебойного питания «POWERCOM Infinity INF-1100».

Характеристики:

Таблица 5.3.3 – Характеристики POWERCOM Infinity INF-1100

|  |  |
| --- | --- |
| Активная мощность | 770 Вт |
| Полная мощность | 1100 Вт |
| Напряжение при питании от батареи | 220-240+/-5%В |
| Время переключения на батареи | 1. мс |

## Проектирование схемы подключения оборудования.

Так как в помещении размещено рабочее место с ПЭВМ, для защиты от косвенного прикосновения оборудовано защитное заземление (зануление) в соответствии с техническими требованиями по эксплуатации.

Для питания ПЭВМ применена система TN (глухозаземленная нейтраль трансформатора). Поэтому, в соответствии с ПУЭ, все открытые проводящие части присоединены к глухозаземленной нейтрали источника питания, то есть используется защитное зануление. В качестве дополнительной меры защиты и для защиты от статического электричества применено дополнительное заземление корпуса ПЭВМ.

Исходя из требований по подключению оборудования, все приборы подключены к сети электропитания следующим образом:

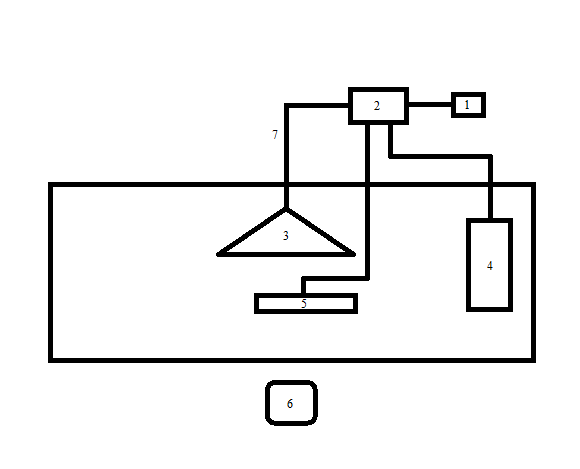


Рисунок 5.4.1 – Схема подключения.

Цифрами на рисунке обозначено следующее:

1)Розетка питания

2)ИБП

3)Дисплей

4)Системный блок ПЭВМ

5)Клавиатура

6)Рабочее место оператора

7)Сетевые кабели питания

Необходимое число розеток – 1 шт.

Системный блок ПЭВМ снабжен навесным замком небольшого размера для защиты от прямого прикосновения токоведущих частей.

## Заключение

В результате выпускной квалификационной работы был разработан комплекс мер по защите конфиденциальной информации на предприятии ООО «Новый мир». Данная система позволяет свести к минимуму угрозы конфиденциальной информации от внутренних источников угроз, то есть сотрудников, работающих в компании. Разработанная система удовлетворяет требованиям законодательства Российской Федерации в области защиты информации.

В ходе ВКР были выполнены следующие задачи:

* рассмотрение угроз информационной безопасности;
* обзор систем обеспечения безопасности конфиденциальной информации;
* разработка системы защиты конфиденциальной информации;
* экономическое обоснование разработанной системы защиты.

## Список использованной литературы

1. ГОСТ 7.32-2017 СИБИД. Отчет о научно-исследовательской работе. Структура и правила оформления.
2. СанПиН 2.2.2/2.4.1340-03. Гигиенические требования к персональным электронно-вычислительным машинам и организации работы.
3. СанПиН 2.2.2.542-96. Гигиенические требования к видеодисплейным терминалам, персональным электронно-вычислительным машинам и организации работы.
4. М.И. Фалеев. Угрозы национальной безопасности государства в информационной сфере, Том №4, 2014. – 55с.
5. Андреева Н.В. Экономика защиты информации: Практикум – Самара: Самар. гос. техн. ун-т., 2019. - 64.
6. Статистика утечек информации, мир –Россия, 2018 [Электронный ресурс]. – URL: https://www.infowatch.ru/company/presscenter/news/15706
7. Установка и настройка прокси-сервера Squid [Электронный ресурс]. – URL: <https://itproffi.ru/ustanovka-i-nastrojka-proksi-servera-squid/>
8. DLP-системы [Электронный ресурс]. – URL: https://inspectsystem.com/articles/dlp-systema-alternativa/?
9. Squid – настраиваем URL – фильтрацию по спискам [Электронный ресурс]. – URL: <https://interface31.ru/tech_it/2013/09/squid-nastraivaem-url-filtraciyu-po-spiskam.html>
10. Документация программы Oracle VirtualBox [Электронный ресурс]. – URL: <https://www.virtualbox.org/manual/UserManual.html>
11. Официальный сайт проекта Ubuntu [Электронный ресурс]. – URL: <https://ubuntu.com/>