**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ**

**Федеральное государственное бюджетное образовательное учреждение высшего образования**

**«Майкопский государственный технологический университет»**

**Факультет информационных систем в экономике и юриспруденции**

**Кафедра информационной безопасности и прикладной информатики**

К защите допускается:

заведующий кафедрой

информационной безопасности и

прикладной информатики

к. техн. н., доцент Чундышко В.Ю.

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

«\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2021г.

**КУРСОВАЯ РАБОТА**

на тему:

**«****РАЗРАБОТКА ПРЕДЛОЖЕНИЙ ПО ЗАЩИТЕ КОММЕРЧЕСКОЙ ТАЙНЫ»**

Направление подготовки 10.03.01 «Информационная безопасность»

Выполнил студент

группы БИ-21 \_\_\_\_\_\_\_\_\_\_\_\_\_\_Д.Р. Козлова

Научный руководитель:\_\_\_\_\_\_\_\_\_\_\_Н.Ш. Козлова

Нормоконтроль пройден «\_\_»\_\_\_\_\_\_\_\_\_\_ 2021 г.

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

(Ф.И.О. нормоконтролера) (подпись)

Майкоп, 2021

**СОДЕРЖАНИЕ**

**ВВЕДЕНИЕ**…………………………………………………………………………..3

**ГЛАВА 1. ИССЛЕДОВАНИЕ ОСНОВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ**

* 1. КОМПЛЕКСНЫЙ ПОДХОД К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ………………………………………………...6

1.2 ИССЛЕДОВАНИЕ СУЩНОСТИ, ЗНАЧЕНИЯ ИНФОРМАЦИИ И СРЕДЫ ФУНКЦИОНИРОВАНИЯ В КОММЕРЧЕСКОЙ ДЕЯТЕЛЬНОСТИ ПРЕДПРИЯТИЯ…………………………………………………………………….13

# ГЛАВА 2. РАЗРАБОТКА МЕРОПРИЯТИЙ ПО ОБЕСПЕЧЕНИЮ СОХРАННОСТИ КОММЕРЧЕСКОЙ ТАЙНЫ

2.1 ПРЕДЛОЖЕНИЕ РЕКОМЕНДАЦИЙ ПО ОБЕСПЕЧЕНИЮ СОХРАННОСТИ КОММЕРЧЕСКОЙ ТАЙНЫ…………………………………..27

* 1. АНАЛИЗ И МОДЕРНИЗАЦИЯ СИСТЕМЫ ЗАЩИТЫ КОММЕРЧЕСКОЙ ТАЙНЫ………………………………………………………………………………36

# ЗАКЛЮЧЕНИЕ……………………………………………………………………49

# СПИСОК ИСТОЧНИКОВ И ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ……..51

# ПРИЛОЖЕНИЯ

# ВВЕДЕНИЕ

**Актуальность.** Информационная безопасность - это очень сложный и долгий процесс, который как правило обеспечивается за счет различных методов и средств организационного, программного и инженерно-технического характера. Как правило, эти методы и средства используют в совокупности, при этом комплекс различных мер обеспечения информационной безопасности образует систему защиты информации. Перед современным бизнесом стоит проблема, сводящаяся к задаче выбора из всего спектра имеющихся решений правильной их комбинации. За счет активного технологического развития в мире, существует и предлагается достаточно много технологий и средств защиты, однако трудность реализации защиты информационной сети организации заключается не в нехватке подходящих технологий, а в выборе из множества возможных решений именно того единственного, которое подойдет лучше всего именно для конкретной сети и требований бизнеса.

Проблемы безопасности состоят в том, что ФСТЭК значительно ужесточила требования к продуктам для обеспечения безопасности, ведет работу по стандартизации процедур создания программного обеспечения (ПО) – приняты два стандарта и еще пять находятся в стадии разработки.

К сожалению, не многие компании, занимающиеся созданием ПО и средств безопасности, внедряют процедуры безопасной разработки. Руководители компаний, которые используют такие процедуры в разработке, сопровождении и документировании программного кода, отмечают, что они дают большой положительный эффект. Компаниям, не применяющим процедур безопасной разработки, гораздо сложнее пройти сертификационные испытания, и сертификация обходится им в целом дороже.

Вызывает обеспокоенность за безопасность аппаратных средств. В последнее время угрозы на аппаратном уровне получили широкое распространение.

Еще одна болевая точка – подготовка кадров. Программы по информационной безопасности в большинстве учебных заведений устарели и не соответствуют современным требованиям. Например, вузы не выпускают специалистов по обеспечению безопасности на аппаратном уровне, практически не готовят юристов в области защиты информации.

Таким образом, актуальность нашего исследования обусловлена недостаточно хорошей организацией режима коммерческой тайны, а также проведением аудита информационной безопасности предприятия.

**Цель работы**: исследовать теоретико- методологические аспекты, защиты коммерческой тайны и разработать мероприятия по ее совершенствованию.

**Задачи** работы:

1. На основе анализа существующих работ определить понятие и сущность коммерческой тайны.

2. Проанализировать деятельность предприятия как субъекта рыночной экономики и носителя коммерческой тайны.

3. Разработать предложения и рекомендации по совершенствованию в организации мероприятий, направленных на сохранение коммерческой тайны.

**Объект исследования** сведения, составляющие коммерческую тайну.

**Предметом исследования** являются меры и средства, обеспечивающие защиту коммерческой тайны.

**Практическая значимость** данной работы заключается в возможности применения полученных результатов непосредственно в процессе деятельности для повышения эффективности, производительности и защищенности.

**Структура** работы определена ее целями и задачами, и включает введение, две главы, заключение, список используемых источников и литературы, а также приложения.

**Во введении** обоснована актуальность исследования, сформулирована цель работы и перечислены задачи, которые необходимо решить.

**В первой главе** рассмотрены сущность, понятие коммерческой тайны и охарактеризованы сведения, которые не могут составлять коммерческую тайну.

**Во второй главе** проведен анализ обеспечения информационной безопасности и выявлены проблемы, также даны рекомендации по разработке организационных мероприятий по обеспечению сохранности коммерческой тайны.

**В заключение** работы сформулированы обобщающие, наиболее значимые результаты работы, подводящие итог, выводы и предложения.

В данной работе использованы материалы предыдущих курсовых работ, научных работ по сходной теме, книги, статьи периодических изданий, переводы оригинальных текстов стандартов, законы, иные нормативные акты, руководящие документы, материалы web–сайтов.

В процессе исследования были использованы труды Корта С.С., Партыка Т.Д., Степанова Е.А., Халяпина Д.Б., Ярочкина В.И., Шиверского А.А., Bye M.A., Морозова В.П.

**ГЛАВА 1. ИССЛЕДОВАНИЕ ОСНОВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ**

* 1. КОМПЛЕКСНЫЙ ПОДХОД К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Информационные системы поддерживают бизнес-процессы и операции, они поддерживают принятие решений сотрудниками и менеджерами и, наконец, поддерживают стратегии конкурентного преимущества. Эти три фундаментальные роли охватывают любые другие роли, которые играют информационные системы в организации.

Информационные системы поддерживают бизнес-процессы и операции организации многими способами. На предприятии, например, учет и обработка информации об продукции и услугах производится с помощью компьютеров и программного обеспечения, что облегчает работу в отличие от традиционного метода использования записных книжек и бумаги для записи такой информации.

Теперь клиенты могут даже сделать свои собственные заказы через вебсайт предприятия, а не посещать лично, чтобы сделать это, что может привести к давлению на персонал предприятия. В настоящее время разработаны системы, позволяющие легко и быстро собирать информацию о клиентах. Теперь, благодаря информационным системам, различные отделы организации работают вместе с легкостью. Служба обслуживания клиентов предприятия теперь может информировать администрацию о том, какие услуги или продукция готовы к использованию, а какие нет, без личного взаимодействия персонала в результате информационных систем. Управление предприятием теперь стало более гладким с хорошо интегрированными информационными системами.

Информационные системы также помогают сотрудникам и менеджерам предприятия принимать обоснованные решения и обладают способностью анализировать данные, собранные как внутри организации, так и из внешних источников, в полезную информацию, которая может быть использована сотрудниками и руководителями в процессе принятия ими решений. Принятие решений является неотъемлемой частью управления и происходит в каждой функции и на всех уровнях. Решения лучше принимать, когда имеется точная информация, которая помогает лицу, принимающему решение, принять объективное решение. Такие типы информационных систем, как управленческие информационные системы, системы поддержки принятия решений и исполнительные информационные системы, специально разработаны для оказания помощи руководству организации в процессе принятия решений. Эти системы генерируют типичные отчеты и графики по таким вопросам, как динамика заказов, анализ клиентов, рентабельность продукции, готовые позиции на складе и прогнозы, отчеты об авариях и невыходах на работу, отчеты об оценке работы и многое другое.

Руководители и сотрудники используют эти отчеты и графики в качестве основы для своих решений. Например, решения о том, какие услуги или продукция должны быть добавлены или удалены из списка покупателя, могут приниматься менеджером по продуктам или услугам после того, как обычно анализ проводится с помощью системы поддержки принятия решений.

Наконец, информационные системы также поддерживают стратегии обеспечения конкурентных преимуществ. Конкуренция в современном бизнесе очень высока, и что станет важным, так это то, как быстро компании смогут преобразовать свои потоки информации, которые они собирают, в знания, чтобы они могли предоставлять услуги и продукты, которые опережают своих конкурентов.

Стратегические информационные системы могут помочь обеспечить производственные операции инновационными средствами, необходимыми для предоставления продуктов и услуг, которые дадут им сравнительное преимущество перед конкурентами. Отмечают, что в индустрии питания и промышленного производства конкурентные преимущества могут привести к увеличению продаж, снижению стоимости товаров (за счет сокращения операционных расходов и менее дорогих каналов распределения), повышению узнаваемости бренда (за счет эффективных рекламных кампаний, ориентированных на соответствующего клиента и доставляемых через наиболее подходящий экономически эффективный способ), хорошим взаимоотношениям между клиентами и организациями (за счет ведения базы данных клиентов и их потребностей) и своевременному принятию эффективных решений.

Все государственные предприятия обязаны хранить информацию, которая может быть повреждена в случае ее уничтожения или получения злоумышленником. Эта информация классифицируется как «секретная», если она предоставляется для государственных учреждений, либо как «коммерческая тайна» или «ценная информация», если она является сведениями для коммерческих предприятий.

Атаки могут осуществляться удаленно, даже из-за границы. Все это создает новые вызовы для ИТ-разработчиков и строителей. Некоторые формы современного предприятия полностью основаны на веб-технологиях (электронная коммерция, IP-телефония и т.д.) и поэтому особенно уязвимы. Существует также необходимость международного сотрудничества в области законодательства и противодействия террористическим сетям. Некоторые протоколы и программы, возможно, потребуется со временем скорректировать в соответствии с требованиями безопасности.

Проблема с системными метриками безопасности состоит в том, что не понимали, как работает сеть. Когда компьютеры объединяются, новые обостряют старые проблемы безопасности. Да, есть формы коммуникации, но локальные сети намного больше, чем WAN. Более высокие скорости передачи и большие линии общего пользования. Блок шифрования может не работать.

Режим конфиденциальности информации, такой как коммерческая тайна, при различных обстоятельствах способствует: получению преимуществ на рынке товаров и услуг (отсюда и увеличение доходов) или иных коммерческих выгод, а также уменьшению расходов. Такие сведения являются большой ценностью для третьих лиц, так как их разглашение может дать выгоду, в том числе преимущество на рынке, другим компаниям.

НСД злоумышленника

уничтожение

искажение

подмена

Рисунок 1.1 Проявление угроз информационной безопасности

Режим конфиденциальности информации подразумевает введение и поддержание на должном уровне особых мер по защите информации.

На защиту конфиденциальной информации могут рассчитывать только зарегистрированные предприниматели, такие как:

* общество с ограниченной ответственностью;
* акционерное общество;
* частные компании, прошедшие процедуру регистрации, внесенные в реестр.

Сведения, составляющие коммерческую тайну, имеют ряд признаков:

* данный вид тайны является потенциально ценной для других организаций;
* доступ к секретной информации может регулировать только ее владелец;
* любая компания имеет возможность оберегать конфиденциальные сведения;
* сведения принадлежат только одной организации и доступ посторонних лиц к ним ограничен;
* зависимость сложности сохранения засекреченной информации прямо пропорциональна ее количеству.

Таким образом, открытое использование информации, составляющей коммерческую тайну, угрожает экономической безопасности любого бизнеса, в связи с этим владелец бизнеса предпринимает меры по сохранению конфиденциальности этой информации и её защите от незаконного распространения и использования. Этот режим имеет четкую классификацию информации, подпадающей под коммерческую тайну.

Кроме этого, к угрозам относится и блокирование информации (нарушение ее доступности), потому что недоступность информации в необходимый момент, как и уничтожение информации, может принести реальный ущерб.

Потенциальная опасность, исходящая от угроз, существует всегда, не зависимо от того реализована она или нет, меняется только её уровень.

Угрозы безопасности информации принято делить на основные виды: преднамеренные и непреднамеренные, которые возникают случайно в процессе работы организации и её сотрудников.

Классификация видов угроз по различным критериям:

* + 1. Угроза информационной безопасности: доступность, целостность, конфиденциальность;
    2. Угрозы могут быть нацелены на следующие компоненты: данные, аппаратура, программы, поддерживающая инфраструктура;
    3. Угрозы по способу осуществления могут быть: случайные либо преднамеренные; природного или техногенного характера;
    4. Угрозы по расположению источника могут быть: внешние, внутренние.

Возможные пути утраты информации, нарушение целостности и конфиденциальности информации. представлены на рисунке 1.2.

Утрата И

переход к III лицу

переход к злоумышленнику

каналы НСД

сотрудник

постороннее лицо

утрата в результате

разглашение человеком

утечка по техническим каналам

организационные

технические

виброакустическийкийй

визуально-оптический

электромагнитный

радиоканал

легальные

аналитическая

обработка

«законной»

информации

нелегальные

нелегальные способы получения И

воровство

продуманный обман

подслушивание

подделка документов

взятничество

шантаж

перехват И

визуальное наблюдение

анализ продукции отходов

Рисунок 1.2 Возможные пути утраты информации (И-Информация)

На рисунке 1.3 приведены основные направления информационной безопасности.

Исходя из выше написанного, можно сказать, что КСЗИ — система, полно и всесторонне охватывающая все предметы, процессы и факторы, которые обеспечивают безопасность всей защищаемой информации [26].

Для более полного рассмотрения КСЗИ необходимо подробней разобрать направления защиты информации.

- нормативно-правовые категории, определяющие комплексные меры защиты информации

НАПРАВЛЕНИЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

- специальные правовые акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе

- регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающая нанесение ущерба

- использование

-средств, препятствующих нанесению ущерба

ПРАВОВАЯ

ЗАЩИТА

ОРГАНИЗАЦИОННАЯ ЗАЩИТА

ИНЖЕНЕРНО-ТЕХНИЧЕСКАЯ ЗАЩИТА

Рисунок 1.3 Направления обеспечения информационной безопасности

Для адекватной защиты коммерческой тайны на предприятии должны быть налажены как организационные, так и инженерно-технические средства защиты информации. В процессе анализа особенностей системы защиты информации и его инженерно-технической и организационной защиты информации были выявлены проблемы, связанные с внутренним порядком и пропускным режимом в организации, данные проблемы оказывают негативное влияние на безопасность конфиденциальной информации, в частности - коммерческой тайны.

Развитие общества находится на таком этапе, который характеризуется возрастанием информационной сферы, она представляет собой совокупность предметов и объектов информации и информатизации, а также системы регулирования общественных отношений, связанных с ней.

Сегодня от обеспечения информационной безопасности зависит национальная безопасность и эта зависимость будет возрастать, поэтому на первый план приоритетных задач во всем мире выходит обеспечение информационной безопасности.

Термин информационная безопасность принято понимать, как состояние защищенность непосредственно самой информации и её носителей от различных видов угроз, источники которых могут быть как преднамеренными - преследующими цель незаконного получения информации, и непреднамеренными - не преследующими цель незаконного получения информации.

1.2 ИССЛЕДОВАНИЕ СУЩНОСТИ, ЗНАЧЕНИЯ ИНФОРМАЦИИ И СРЕДЫ ФУНКЦИОНИРОВАНИЯ В КОММЕРЧЕСКОЙ ДЕЯТЕЛЬНОСТИ ПРЕДПРИЯТИЯ

На сегодняшний день решение проблемы обеспечения экономической безопасности субъектов рыночных отношений является первоочередной задачей не только для государства, но и для предприятий. Нестабильные условия российской экономики заставляют непрерывно искать пути поддержания функционирования организации, равно как и снижения появления перманентно возникающих угроз.

Предприятия не относятся к самой уязвимой группе хозяйственных субъектов, но также, как и другие организации нуждаются в эффективной системе, обеспечивающей всестороннюю безопасность.

Прежде чем раскрыть взаимосвязь между и субъектом и объектом экономической безопасности необходимо дать определение понятию «предприятие» и выявить его особенности [14].

Предприятие - это основная единица экономической системы любого государства. Его первоочередная задача удовлетворение потребностей общества в продукции или оказании услуг. В большинстве случаев представляет собой завод, комбинат, фирму, фабрику. Несмотря на существование различных отраслей, можно выделить следующие признаки предприятия:

* особая форма управления: действия координируются с целью достигнуть соответствия частей целого;
* в большинстве случаев является градообразующим предприятием;
* в структуре актива баланса преобладают внеоборотные активы;
* обеспечивают государственные нужды и могут иметь доступ к государственной тайне;
* реализуют произведенный товар от своего имени [13].

Учитывая все вышеперечисленные особенности, стоит отметить, что обеспечение экономической безопасности в данном случае представляет собой прогнозирование и последующую разработку мер по противодействию возможным угрозам. Из этого утверждения логически следует, что главная задача этой сложной системы заключается в предотвращении негативных воздействий, не допуская непосредственного проникновения вредоносных элементов внешней экономической среды. Необходимость защиты на ранних этапах возникает по причине значительности такого типа предприятий не только для потребителей, но и на государственном уровне.

Таким образом, экономическая безопасность предприятия - многоцелевая система, которая вопреки текущему финансовому положению организации, призвана свести к минимуму воздействие внутренних и внешних факторов, окружающей его экономической среды [20].

На данный момент в среде ученых проблема обеспечения экономической безопасности предприятий не нашла единства взглядов. Этот факт не уменьшает потребности в разработке системы принципов организации экономической безопасности. Необходимость является следствием того, что в превалирующем количестве случаев предприятие - финансовая основа экономики региона, крупнейшие из них до сих пор остаются градообразующими. Таким образом, экономическую безопасность предприятий можно приравнять к фундаменту экономической безопасности региона.

Многие предприятия работают на обеспечение государственных нужд, именно поэтому они являются основной единицей экономики страны. Выигрывая тендеры или, являясь естественными монополистами, они могут в последствии получить доступ к государственной тайне. Также предприятия - держатели коммерческой тайны, это не только вопрос о базовой защите интеллектуальной собственности, но и о наличие особой системы доступа к различным разработкам.

Под пунктом внеоборотные и оборотные активы подразумевается особая защищенность денежных средств, запасов, а также основных средств: зданий, сооружений, многолетних растений, оборудование, машины, транспорт.

Для обеспечения их безопасности необходимо выполнять следующие действия:

* уменьшить количество несанкционированного самовывоза оборудования с территории предприятия, путем более качественного контроля и разработать план производства продукции таким способом, который бы позволил максимально эффективно использовать оборудование по его целевому назначению;
* обеспечить подбор квалифицированного персонала, чтобы снизить вероятность нанесение ущерба объектам основных средств;
* наличие договоров материальной ответственности с персоналом который непосредственно взаимодействует с оборудованием [26].

Элемент «денежные средства» подразумевает не только наличные денежные средства в кассе организации, но и выручку, внереализационные доходы, а также инвестиции.

Меры, обеспечивающие экономическую безопасность предприятия:

* контроль за поступлением денежных средств, их последующем распределением и использованием;
* наличие специально оборудованного помещения, где находится кассовый аппарат и кассир;
* проведение внеплановых проверок в кассе [23].

Персонал организации как объект защиты является одним из самых сложных, так как человеческое поведение невозможно спрогнозировать, а соответственно предотвратить негативные ситуации. Немаловажно в данной ситуации подойти к кадрам не только как к источнику угроз, но и как к возможной мишени для злоумышленников. Для того чтобы обеспечить необходимую лояльность работников, организация должна выполнять следующие требования:

* достойная оплата труда, согласно выполняемому объему работ и квалификации;
* наличие выплат социального характера;
* обеспечение безопасности труда, включая материальную ответственность предприятия;
* комфортные условия для выполнения работы.

Информационные ресурсы - один из важнейших компонентов предприятий. Зачастую схемы, чертежи и разработки по своей стоимости эквиваленты оборудованию. Связи с этом необходимо обеспечить особый доступ к таким документам. Санкционирование возможном путем создания структуры, которая разобьет персонал на группы с различным уровнем доступа к секретной информации [30].

Система обеспечения экономической безопасности имеет зависимость от ряда факторов. Например, объем производства, финансово-хозяйственная деятельность, изношенность основных средств, кадровые ресурсы. Значение этих показателей коррелируют с количеством средств для обеспечения непрерывной работы службы экономической безопасности. Также её функционирование должно быть определенно нормативно-правовыми актами, в которые будут включены следующие пункты: документы, определяющие статус подразделения, нормы, задачи, полномочия, обязанности, средства и методы.

Информационное обеспечение подразумевает своевременное получение необходимых сведений, для принятия оперативных решений. Информация должна быть объективной, достаточной и иметь документальное подтверждение [34].

Организационное обеспечение – комплекс мер, направленных на плановое обеспечение потребностей производства и предотвращение возможных инцидентов. Нормативно-правовые документы и сотрудники контролирующих подразделений регулируют соблюдение норм и правил, описанных во внутренней распорядительной документации предприятия.

Кадровое обеспечение регулируется деятельностью отдела кадров. Он отвечает за сбор и регистрацию данных о соискателях вакансий на предприятии. При трудоустройстве соискателем заполняется анкета, где соискатель указывает сведения о себе. После заполнения анкеты, претендент на вакансию проходит медицинское обследование у необходимых специалистов (определяется исходя из ст. 212, 213 ТК РФ). В случае утвердительного решения о приеме на работу и отсутствия противопоказаний врача с ним проводят инструктажи по охране труда, пожарной безопасности, внутри объектовому режиму. После чего, уже в рабочее время внутри подразделения проводятся дополнительные локальные инструктажи отдела, необходимые для работы.

На первом этапе проводится подбор специалистов на должность, которые должны отвечать не только требованиям квалификации, но и пройти проверку службы безопасности (наличие вредных привычек, судимостей, кредитов и т.д.). Следующий этап - это непосредственная работа с сотрудниками: обеспечение психологически комфортной обстановки, повышение квалификации, также разработка системы мотивации для лучшей отдачи. Завершающий этап - увольнение. Работники кадровой службы, должны обладать знаниями о проведении этой процедуры согласно трудовому кодексу [35].

На любом предприятии хранятся и обрабатываются сведения, составляющие коммерческую тайну. Они зафиксированы в перечне сведений коммерческого характера ограниченного распространения Основными сведениями, составляющие коммерческую тайну, согласно перечню, являются:

* производственная информация: сведения о свойствах и характеристиках материалов и комплектующих изделий, сведения о состоянии производства, сведения о подготовке производства к выпуску новой продукции, сведения о рецептуре материалов, разработанных на предприятии и являющихся собственностью предприятия, сведения о конструкторско-технологических разработках;
* финансовая информация: перечень действующих договоров по выпуску продукции, сведения о производственных мощностях предприятия, сведения об объемах выпуска продукции в натуральном и денежном выражении, сведения о кредитах и долговых обязательствах предприятия, аналитические отчеты об итогах и перспективах реализации продукции, сведения о себестоимости вновь разрабатываемых изделий;
* научно-техническая информация: сведения о методах защиты от подделки продукции и товарного знака предприятия, сведения о патентоведческих исследованиях в области научно-технических, опытно-конструкторских работ, информация оформления патентных формуляров на изобретение;
* информация, составляющая коммерческую тайну сторонних организаций, полученная в ходе деятельности предприятия.

Техническое обеспечение характеризуется наличием и использованием технических средств, направленных на защиту активов предприятия. Сюда можно включить контрольно-пропускной пункт, камеры, сейфы, сигнализации.

Нормативно-правовое обеспечение – комплекс документов, регламентирующих работу службы. Она должна опираться на текущее законодательство, а также на разработанные внутри организации нормативы.

Организационная структура системы экономической безопасности предприятий представлена на рисунке 1.4.

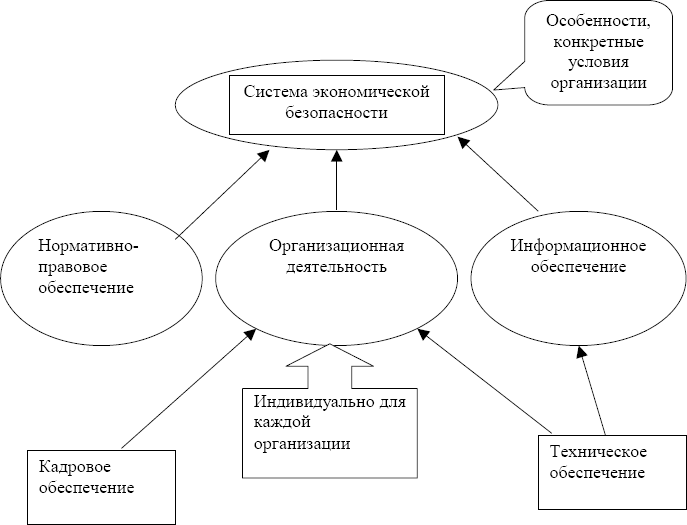


Рисунок 1.4 Система экономической безопасности

Эффективное функционирование модели экономической безопасности невозможно без взаимодействия администрации предприятия и сотрудников. Деятельность обоих групп должны быть организованна в соответствии с регламентом работы. Основные направления исполнения мероприятий должны основываться на следующих принципах:

* законность;
* баланс между интересами государства и предприятия;
* взаимная ответственность администрации организации и сотрудников;
* сотрудничество с органами, реализующими концепцию национальной безопасности.

Обеспечение экономической безопасности предприятий не сводиться лишь к разработке и проведению мероприятий. Оно представляет собой непрекращающийся многоцелевой процесс, который заключается в:

* непрерывном мониторинге возможных угроз;
* соответствии персонала разработанной системе требований по уровню его профессиональной подготовки;
* перманентном контроле за предприятием, а также создание группы, которая могла бы осуществлять внутренний контроль;
* совершенствовании службы экономической безопасности предприятия;
* использовании средств технического обеспечения по их целевому назначению, не допуская простоя [38].

Таким образом, при обеспечении экономической безопасности для начала выделяют объекты, нуждающиеся в первоочередной защите. Они представляют собой различные источники, с помощью которых предприятие может достигнуть финансового успеха. В дальнейшем производят мониторинг степени защищенности организации, цель данного мероприятия выявить слабые стороны и возможные угрозы. Они систематизируются относительно источника возникновения, вероятности наступления, по возможности прогнозирования и по объектам посягательства. После выявления слабых сторон, служба тестирует различные способы и приемы для предотвращения возможного ущерба.

Следующий пункт - запуск системы обеспечения экономической безопасности. Её деятельность опирается на принципы, установленные компанией, а деятельность регламентирована нормативно-правовыми актами. Результаты деятельности анализируются специалистами службы, оценивается эффективность работы, в случае необходимости производятся изменения и доработки [30].

Причина, по которой экономической безопасности предприятия, уделяется такое внимание - её влияние на ряд индикаторов экономической безопасности региона.

Необходимо отметить, что система обеспечения экономической безопасности не заключается лишь в предотвращении ущерба. Являясь многоцелевой системой в её основные задачи, входит работа по оптимизации финансово-хозяйственных процессов. Например, планирование распределения денежных потоков, планирование выпуска продукции, расчет пороговых значений экономических показателей.

Самым главным пунктом перераспределения доходов и расходов предприятия - расчет финансовых ресурсов на обеспечение системы экономической безопасности. Этот тезис подразумевает, что для максимального сдерживания угроз организация нуждается в денежных средствах, то есть чем выше уровень экономической безопасности, тем больше финансирования требуется. Сюда включаются не только затраты по реализации и разработке мероприятий, но и оплата труда сотрудникам, которые задействованы в них, содержание технических средств защиты. Таким образом, промышленному предприятию необходимо найти баланс между уровнем экономической безопасности и расходами на содержание [28].

Можно считать, что финансовая служба в силу обычно осуществляемых ею функций фактически задействована в обеспечении экономической безопасности предприятия. Среди этих функций стоит особо выделить следующие: обеспечение учета и контроля движения денежных средств, иных товарно-материальных ценностей, а также текущего контроля доходов и расходов, проведение инвентаризаций, сверок расчетов с дебиторами и кредиторами. Контроль за качеством исполнения этих функций может быть возложен на службу внутреннего контроля или внутреннего аудита, а также на контрольные органы организации, созданные в соответствии с действующим законодательством.

Внешний аудитор также может давать оценку качества работы финансовой службы. Как правило, сотрудники этих служб, а также внешние аудиторы обладают достаточной квалификацией, чтобы выполнить такую работу на должном уровне. Казалось бы, для вмешательства службы безопасности организации в эти вопросы нет никакой необходимости. Однако есть один важный момент, который может быть для нее все-таки интересен. Дело в том, что те, кто осуществляет контроль за деятельностью финансовой службы, в силу специфики вопроса почти всегда имеют возможность манипулировать полученными результатами, а также оказывать определенное влияние на деятельность этой службы.

Может сложиться ситуация, когда финансовая служба исполняет свои обязанности не на надлежащем уровне даже при организации контроля за ее деятельностью, что представляет угрозу для экономической безопасности предприятия.И здесь следует обратить особое внимание на то, кому фактически подчиняются контролирующие лица или службы. Встречаются ситуации, когда контролирующие лица входят в состав финансовой службы, подчиняются начальнику финансовой службы (заместителю директора по экономике и финансам, финансовому директору, вице-президенту по экономике и финансам др.).

В таких случаях речь идет уже не об относительно независимом контроле, а о самоконтроле финансовой службы. При этом создается определенная почва для злоупотреблений внутри финансовой службы, и из элемента обеспечения экономической безопасности организации она сама может (хотя совсем необязательно) превратиться в источник угрозы. Таким образом, для успешного использования финансовой службы в качестве элемента обеспечения экономической безопасности организации должны быть созданы определенные условия.

Финансовая служба как источник информации для службы безопасности. Обычно большинство данных, с которыми работает финансовая служба, имеются в корпоративных информационных системах, программах учета, программах документооборота, иных базах и доступны работникам других служб. Однако следует помнить, что у финансовой службы скапливается много информации, которая никак не отражается в упомянутых системах и программах, но может иметь ценность для службы безопасности организации.

Приведем пример. Не секрет, что существует практика «откатов», когда сотрудники организации обеспечивают контрагентам особые условия и получают от них благодарность. Рассмотрим два этапа, в которые можно выявлять «откатные» явления без больших дополнительных усилий. На первом этапе, когда появляется контрагент и происходит заключение с ним договора, целесообразно задокументировать, кем из работников и каким путем устанавливается контакт с контрагентом.

Можно внести соответствующие графы в лист согласования договора либо получать эту информацию от представителей юридической или финансовой службы. Наличие подобной графы может оказать некоторое сдерживающее действие на работников организации. Информация от юридической или финансовой службы о том, кто «активничал» при заключении договора, позволит проверить достоверность сведений, внесенных в лист согласования, и, возможно, сразу взять объект «на карандаш».

Второй этап – это работа по договору. Бывает, что сотрудник, практикующий «откаты», не проявляет осторожность или утрачивает ее ввиду безнаказанности и начинает «хлопотать» внутри своей организации об «откатном» контрагенте. Он может обращаться в финансовую службу с целью узнать, оплатили ли определенному контрагенту счет или когда он будет оплачен, а также с просьбой об ускорении или приостановке (в случае возможности) оплаты счета.

Если такие обращения не входят в круг должностных обязанностей сотрудника либо становятся в отношении одного из контрагентов излишне частыми, настойчивыми, странными, то эта информация может стать для службы безопасности основой для размышлений и дальнейших действий. Как уже было отмечено, на финансовую службу в целом и отдельных ее сотрудников может оказываться давление как извне, так и изнутри организации, причем последнее случается гораздо чаще. Внутри организации это могут быть внешне вполне правомерные приказы, распоряжения, инструкции, устные указания.

Также в отдельных случаях угрозы могут прикрываться личностными взаимоотношениями. Вот типичный вариант: излишне строгий начальник, не дающий спуску своим подчиненным, придирается ко всяким мелочам, кричит по поводу и без повода на своих сотрудников. Подобное поведение, как правило, является источником угрозы для экономической безопасности всей организации, даже если это позволяет себе финансовый или генеральный директор.

Поэтому информация о подобных действиях в отношении финансовой службы должна быть «тревожным сигналом» для службы безопасности компании. Исходя из сказанного, а также из иных соображений, не вошедших в данную работу, можно сделать вывод о том, что взаимодействие с финансовой службой может повысить эффективность деятельности службы безопасности.

Исходя из вышеизложенного, можно сделать вывод о том, что взаимодействие с финансовой службой может повысить эффективность деятельности службы безопасности план такого взаимодействия может выглядеть следующим образом:

* + 1. Определение основных угроз экономической безопасности организации.
    2. Разработка системы показателей основных угроз.
    3. Установление каналов получения информации по показателям основных угроз от финансовой службы.
    4. Разработка системы мероприятий реагирования на изменения показателей. Под системой показателей мы в данном случае понимаем набор определенных данных и правил их обработки. Специфика работы финансового отдела требует привлечения опытных сторонних специалистов финансовой сферы (аудиторов, экономистов, бухгалтеров и др.) для разработки системы показателей.

Примерная структура системы показателей по финансовой службе может включать в себя несколько групп. Группа организационных показателей:

* подчиненность (лояльность) ключевых сотрудников финансовой службы;
* подчиненность (лояльность) лиц, контролирующих деятельность финансовой службы;
* степень обеспеченности финансовой службы персоналом;
* факты (попытки) изменения организационной структуры финансовой службы.

Группа управленческих показателей:

* функциональная подчиненность сотрудников финансовой службы; формализация бизнес-процессов, наличие должностных инструкций, регламентов;
* факты (попытки) изменения, нарушения бизнес-процессов. Группа фактических показателей:
* факты (попытки) вовлечения сотрудников финансовой службы в сомнительные действия;
* факты (попытки) намеренной, целенаправленной компрометации

сотрудников финансовой службы;

* факты (попытки) давления в целях сокрытия хищений ТМЦ, денежных средств;
* факты (попытки) давления в целях искажения результатов финансово-хозяйственной деятельности организации;
* факты (попытки) использования финансовой службы как источника информации.

Группы косвенных показателей:

* исключение финансовой службы из ряда бизнес-процессов;
* сокращение численного состава работников финансовой службы и создание таких условий, когда они ежедневно перегружены работой;
* усложнение либо чрезмерное упрощение документооборота;
* излишнее усложнение либо чрезмерное упрощение системы учета в организации;
* наделение финансовой службы несвойственными ей функциями;
* использование фактора времени для оказания давления на финансовую службу;
* поведение сотрудников, особенно руководителей, выходящее за рамки общепринятой деловой этики.

Группа специальных (индивидуальных для каждой организации) показателей, например:

* постоянная пересортица товара, выявляемая при инвентаризациях;
* чрезмерно частые обращения менеджера по закупкам к информации об оплатах отдельному поставщику.

Подводя итог, можно обозначить, что экономическая безопасность предприятия - это особенная, не похожая на другие, система, направленная на сдерживание угроз на оптимальном уровне, вместо их искоренения. Также её задачей является внутреннее переустройство организации для получения лучшего финансового результата.

В процессе проведения анализа существующей системы защиты коммерческой тайны были выявлены объекты защиты, были получены сведения, необходимые для составления перечня угроз и рекомендаций по их устранению в виде модернизации системы защиты коммерческой тайны. А также описан ряд мер и список организационно-распорядительной документации, необходимой для сопровождения режима коммерческой тайны в должном порядке.

Результатом второй главы будет перечень приоритетных к устранению угроз, с помощью которого будут подобраны рекомендации по модернизации системы защиты коммерческой тайны.

# ГЛАВА 2. РАЗРАБОТКА МЕРОПРИЯТИЙ ПО ОБЕСПЕЧЕНИЮ СОХРАННОСТИ КОММЕРЧЕСКОЙ ТАЙНЫ

2.1 ПРЕДЛОЖЕНИЕ РЕКОМЕНДАЦИЙ ПО ОБЕСПЕЧЕНИЮ СОХРАННОСТИ КОММЕРЧЕСКОЙ ТАЙНЫ

Информация, составляющая коммерческую тайну, защищается в соответствии с введенным режимом коммерческой тайны, который регулирует Положение о защите коммерческой тайны. Отсутствующие части в Положении, необходимо восполнить и переработать имеющиеся для полноценного функционирования режима защиты коммерческой тайны.

Необходимо составить список документации для разработки и внедрения, а именно:

1. Граница ответственности лиц, ознакомленных с информацией, составляющей коммерческую тайну.
2. Список лиц, допущенных к информации, составляющей коммерческую тайну.
3. Порядок установления и снятия грифа «Коммерческая тайна».

Помимо документального сопровождения, требуется ввести организационные меры по оформлению допуска лиц к информации, составляющей коммерческую тайну, усилению контроля доступа к серверному помещению и контролю доступа в режимные подразделения.

На предприятии осуществляется комплекс мер по защите информации, обрабатываемой в информационной системе. По результатам составленной модели угроз были выявлены актуальные угрозы, защищенность от которых необходимо повысить. Поэтому предлагается ряд мер, для повышения уровня защищенности от возможных угроз.

С целью повышения защищенности от угроз, рекомендуется ввести определенные организационные меры:

1. Проведение информирования об обновлении законодательства в сфере информационной безопасности.
2. Проведение плановых осведомлений об ответственности за нарушение законодательства, уставов и политик предприятия с приведением статистики по произошедшим инцидентам.
3. Оснащение окон кабинетов сотрудников, находящихся на первом этаже заводоуправления металлическими решетками.
4. Оснащение серверного помещения стационарными RFID- считывателями, по типу уже установленных в некоторых подразделениях предприятия.
5. Оснащение режимных подразделений турникетов с RFID считывателем, по типу уже установленных на предприятии.

Предполагается, что данные меры инструктажа позволят повысить информированность, дисциплинированность и ответственность сотрудников предприятия и снизить частоту возникновения инцидентов информационной безопасности. Эти меры, направленные на контроль доступа в режимные и серверные помещения, позволит ограничить угрозы утечки видовой информации.

На предприятии реализовано ограничение прав пользователей на установку стороннего программного обеспечения. Такими правами обладают администраторы информационной безопасности, администраторы вычислительной сети и сотрудники подразделения по техническому обслуживанию вычислительной техники.

Для повышения защищенности системы от возможных программных уязвимостей, вредоносного ПО, рекомендуется ограничить права на выполнение сторонних исполняемых файлов-инсталлеров и скриптов средствами ОС Windows. Распространить права рекомендуется только на администраторов информационной безопасности. А также обеспечить документирование данной процедуры путем запроса на установку стороннего программного обеспечения через служебную записку и акт установки программного обеспечения, оформляемый администратором. В связи с реорганизацией обязанностей администраторов необходимо разработать обновленную инструкцию. Соответствующие образцы документов были разработаны и готовы к внедрению (приложения).

Защита информации на предприятии должна осуществляться специалистами отдела службы безопасности, деятельность которых курируют заместитель генерального директора и сам генеральный директор. Распорядительная документация основывается на требованиях ФСТЭК России и ФСБ России.

Защита информации на предприятии должна осуществляться организационными методами (инструктаж о порядке обработки конфиденциальной информации), физической развязкой внутренней (ЛВС) и внешней (Интернет) сетями, дополнительно для защиты канала связи с сетью Интернет применяется межсетевой экран, для предотвращения НСД в ЛВС и автономные ПЭВМ используются программные возможности ОС Windows (с применением парольной политики), прокладка линий связи ЛВС по территории предприятия в подземных коммуникациях или путем подвеса на высоте более 3 метров, прокладка линий связи ЛВС предприятия по корпусам в кабельных лотках, закрепленных между фальш-потолком и потолком.

Правовое обеспечение должно быть направлено на разработку и внедрение нормативно-правовой документации, призванной обеспечить предприятие возможностями для ведения деятельности в рамках правового поля. Комплекс мероприятий по внедрению используемых документов на предприятии будет реализован для достижения следующих целей:

* разработки нормативно-правовой базы;
* анализа и изменения уставных и учетных документов;
* получения лицензий и разрешений для осуществления установленных видов деятельности.

На предприятии необходимо разработать и внедрить необходимую нормативно-правовая документацию, регулирующую взаимоотношения подразделений, границы обязанностей и ответственности. Основные положения деятельности предприятия, закреплены в Уставе. Необходимы лицензии на осуществление деятельности по защите информации в следующих областях:

* проведение анализа организации обеспечения информационной безопасности и режима секретности;
* разработка руководящих документов предприятия по режиму, технической защите информации (руководство по защите информации, , инструкции по внутри объектовому режиму и т.д.);
* проведение аттестации объектов информатизации (технических средств передачи и обработки информации, выделенных (защищенных) помещений для проведения закрытых совещаний и т.д.);
* проведение специальных мероприятий по обнаружению устройств негласного съема информации (закладок) в помещениях и технических средствах;
* проведение специальных исследований технических средств передачи и обработки информации (ПЭВМ, средства связи, средств хранения информации и т.д.);
* разработка проектов экранированных сооружений, безэховых камер, выделенных и защищаемых помещений;
* подбор, закупка, монтаж, настройка и сервисное обслуживание средств технической защиты информации;
* подбор, закупка, монтаж, настройка и сервисное обслуживание криптографических устройств;
* проведение аттестации экранированных сооружений, безэховых камер и рабочих мест по требованиям.

На основании анализа было выявлено, что источниками информации, являющимися коммерческой тайной, а, следовательно, потенциальными источниками утечки в организации являются:

1. Документация предприятия (входящие-исходящие, приказы, бизнес-планы, деловая переписка и т.п.). Разнообразие форм и содержания документов по назначению, направленности, характеру движения и использования является весьма заманчивым источником для злоумышленников, что, естественно, привлекает их внимание к возможности получения интересующей информации.

Несмотря на то, что не всякий документ содержит коммерческую тайну, необходимость в их учете, тем не менее, существует. Не бывает важных и не важных документов. Любой, даже самый малозначительный документ, при определенном стечении обстоятельств может оказаться чрезвычайно важным. Организация контроля за документацией позволит избежать путаницы и неразберихи в дальнейшем, ведь, работа любого предприятия связана с огромным объемом рабочих документов. Кроме того, надлежащая система учета и контроля предотвратит многие проблемы, причем не, только из области безопасности. Известны многочисленные случаи, когда утеря или случайное уничтожение финансовых и деловых документов наносила колоссальный ущерб предприятию.

Обобщенно систему контроля и учета документов необходимо представить в следующем виде:

1. Учет всей документации предприятия с классификацией по сфере применения, дате, содержанию и т.п.

2. Регистрация и учет всех входящих/исходящих документов предприятия с фиксацией в специальном журнале информации о дате получения/отправления документа, откуда поступил, или куда отправлен, классификация (письмо, счет, договор, приглашение и т.п.).

3. Регистрация документов, с которых делаются копии с фиксацией в специальном журнале (дата копирования, количество копий, для кого или с какой целью производятся копии и т.п.).

4. Особый режим уничтожения документов. Перед уничтожением документов необходимо проконтролировать их содержание во избежание случайного уничтожения нужных документов. Важно, чтобы документы не просто выбрасывались в корзину, а предварительно измельчались при помощи «шредера» (уничтожителя бумаги) или вручную таким образом, чтобы их невозможно было бы восстановить. Документы, имеющую особую ценность, после измельчения целесообразно сжечь. Об уничтожении документов в обязательном порядке составляется акт, который подписывается ответственным лицом, а также лицами присутствующими при уничтожении.

Для облечения системы «контроля» все документы следует разделить на три категории: документы общего пользования; документы для служебного пользования; документы секретного характера.

Различные категории документов отличаются друг от друга не только назначением, но и кругом лиц, имеющих доступ к ним. Каждой категории необходимо присвоить свой гриф. Это можно сделать при помощи штампов, специальных отметок, а можно и просто при помощи цвета (например, документы общего пользования - белого цвета, документы служебного - желтые, а секретные - красного).

Важно, чтобы эта система была реализована и успешно применялась. Для этого необходимо провести соответствующую разъяснительную работу с персоналом, а также провести необходимый инструктаж.

Работу по контролю за документами поручить отдельному сотруднику - секретарю, однако в идеале этим должна заниматься группа режима службы безопасности.

Кроме того, целесообразно также принятие соответствующего положения регламентирующего режим документооборота предприятия. В данном положении необходимо отразить правила работы с документами, а также особенности работы, с документацией носящей конфиденциальный характер. На анализируемом предприятии этот документ только в разработке.

К любому исчезновению или уничтожению документов, особенно содержащих важную информацию, необходимо отнестись со всей серьезностью. В этом случае, в обязательном порядке на предприятии проводится внутреннее расследование. Результаты расследования анализируются, если необходимо, лица, виновные в утере документов, привлекаются к дисциплинарной ответственности, а в необходимых случаях лишаются доступа к документам, содержащих коммерческую тайну. Важно, чтобы расследование не стало формальностью, а из его результатов были сделаны надлежащие выводы и допущенные ошибки исправлены в максимально короткое время.

Кроме того, случаи утери или уничтожения документов в дальнейшем могут использоваться в качестве примера при инструктаже сотрудников и работе службы безопасности.

В организации должна вестись регистрация и учет всех входящих/исходящих документов предприятия с фиксацией в специальном журнале информации о дате получения/отправления документа, откуда поступил, или куда отправлен, классификация (письмо, счет, договор, приглашение и т.п.).

Необходимо применять следующие правила предосторожности при работе с документами:

* не надо делать ненужных копий документов;
* черновики и наброски секретных документов должны быть уничтожены;
* секретные документы хранятся отдельно от остальных, в изолированном помещении с ограниченным доступом в сейфе;
* копировальная техника не находится в одном помещении с документами, представляющими коммерческую ценность для того, чтобы исключить их несанкционированное копирование;
* нельзя оставлять документы на рабочем месте без присмотра, даже на короткое время;
* нельзя, чтобы посторонние лица читали рабочие документы, находящиеся на столе или в кабинете работника. При появлении постороннего лица документы должны быть убраны в хранилище, шкаф, ящик стола;
* установлен запрет на вынос работниками документов за пределы предприятия без предварительного разрешения лица, ответственного за сохранность коммерческой тайны.

2. Рабочий персонал или просто люди (в это понятие входят все без исключения работники предприятия, в том числе и сам директор).

3. Партнеры, контрагенты или клиенты, пользующиеся или пользовавшиеся услугами, являются наиболее осведомленными источниками, зачастую обладающими важнейшими секретами. Поэтому они заслуживают отельного внимания при анализе системы защиты.

4. Производимая продукция или оказываемые услуги.

5. Технические средства обеспечения производственной деятельности.

6. Косвенные источники (мусор, реклама, публикации в печати).

В организации не разработаны до конца и не утверждены следующие документы, обеспечивающие сохранность коммерческой информации:

1. Перечень сведений, составляющих коммерческую тайну.
2. Положение о коммерческой тайне.
3. Инструкция по обеспечению сохранности коммерческой тайны.
4. Обязательство о неразглашении коммерческой тайны, контракт о допуске к конфиденциальной информации (Приложение 8).
5. Памятка работнику о сохранении коммерческой тайны (Приложение 9).
6. Специальные обязанности лиц, допущенных к сведениям, составляющим коммерческую тайну.
7. Контракт о допуске к коммерческой тайне (приложение к трудовому договору) или соглашение о неразглашении информации, составляющей коммерческую тайну.
8. Список сотрудников, имеющих доступ к информации, составляющей коммерческую тайну.
9. Порядок установления и снятия грифа «Коммерческая тайна».
10. Пример заявки на период отпуска/болезни сотрудника.
11. Пример заявки на возвращение сотрудника после болезни.

Необходимо разработать все эти документы, образцы представлены в приложениях работы.

Следует разработать Положения о коммерческой тайне и режиме обеспечения коммерческой тайны, в части касающейся каждого сотрудника, необходимо доводить до каждого сведения непосредственным руководителем.

Разглашение коммерческой тайны или неосторожное обращение со сведениями, составляющими коммерческую тайну, может нанести ущерб. Все сотрудники обязаны строго хранить сведения, отнесенные к коммерческой тайне и соблюдать порядок обращения со сведениями (материалами), составляющими её. Разглашение коммерческой тайны, передача третьим лицам сведений, составляющих коммерческую тайну, публикации каких-либо сведений о предприятии без предварительного согласия администрации, а также использование сведений, составляющих коммерческую тайну, для занятия любой деятельностью, которая в качестве конкурентного действия может нанести ущерб Обществу, влечет гражданско-правовую ответственность, предусмотренную нормами действующего законодательства.

При участии в работе сторонних организаций сотрудник может знакомить их представителей со сведениями, составляющими коммерческую тайну, только с разрешения непосредственного руководителя структурного подразделения предприятия. При этом руководитель должен определить конкретные вопросы, подлежащие рассмотрению, и указать, кому и в каком объеме может быть сообщена информация, подлежащая защите.

Необходимо запретить помещать без необходимости сведения, составляющие коммерческую тайну, в документы открытого характера. Такое нарушение порядка обращения со сведениями, составляющими коммерческую тайну, рассматривать как их разглашение и сотрудники должны нести ответственность в соответствии с установленным порядком.

Об утрате или недостаче документов, изделий, содержащих коммерческую тайну, удостоверений, пропусков, ключей от режимных помещений, хранилищ, сейфов, металлических шкафов, личных печатей, а также о причинах и условиях возможной утечки таких сведений сотрудник обязан немедленно сообщить уполномоченному лицу.

При увольнении, перед уходом в отпуск, отъездом в командировку или предполагаемым отсутствием на рабочем месте в течение более или менее длительного срока сотрудник обязан сдать уполномоченному лицу предприятия все носители коммерческой тайны (рукописи, черновики, документы, чертежи, магнитные ленты, дискеты, распечатки на принтерах и т.д.), которые находились в распоряжении сотрудника в связи с выполнением им служебных обязанностей.

Сотрудник обязан по первому требованию уполномоченного лица предъявить для проверки все числящиеся за ним материалы, содержащие коммерческую тайну, представлять устные или письменные объяснения о нарушениях установленных правил выполнения работ, учета и хранения документов и т.д., фактов разглашения коммерческой тайны, утраты документов, содержащих коммерческую тайну.

В случае попытки посторонних физических или юридических лиц получить информацию, составляющую коммерческую тайну, сотрудник обязан сообщить об этом директору.

Срок действия ограничений, связанных с необходимостью защиты коммерческой тайны, совпадает со сроком действия контракта с сотрудником. Обязательства по обеспечению сохранности коммерческой тайны содержатся в Трудовом договоре Сотрудника. Заключение (подписание)

Таким образом, для более эффективной организации работы по защите коммерческой информации весьма целесообразно разработать и утвердить Положение о коммерческой тайне. Этот документ основывается на действующем законодательстве и отражает специфику данного субъекта предпринимательства. Он должен включать перечень сведений, составляющих коммерческую тайну, степень конфиденциальности информации, порядок доступа к информации и круг работников предприятия, допущенных к информации той или иной степени конфиденциальности.

* 1. АНАЛИЗ И МОДЕРНИЗАЦИЯ СИСТЕМЫ ЗАЩИТЫ КОММЕРЧЕСКОЙ ТАЙНЫ

В Российской федерации основным законом, регламентирующим отношения с информацией, составляющей коммерческую тайну является федеральный закон № 98 «О коммерческой тайне», который был разработан и внедрен в действие29.07.2004 г. Он устанавливает понятие коммерческой тайны и право на ее сохранность.

209-ФЗ «О развитии малого и среднего предпринимательства» также имеет положения, касающиеся информации, составляющей коммерческую тайну. Статья 5 регламентирует предоставление сведений, составляющих коммерческую тайну. Держатель обязан по требованию органов государственных властей либо муниципальных, предоставить сведения, входящие в понятие коммерческой тайны. Прошение должно быть удостоверено подписью должностного лица, с определением права и цели запроса сведений, и период их подачи, если он не регламентирован законодательством;

Если держатель данных отказывается предоставлять информацию органам государственной власти или муниципальным органам, они имеют основание запросить их через суд;

Держатель коммерческой тайны и государственные органы, и иные организации, имеющие доступ к коммерческой тайне, обязаны предоставить сведения по требованию судебных инстанций, следственных и спецслужб, по системе и праву, прописанным в законах РФ.

На акты, где указана коммерческая тайна, наносится отметка «Коммерческая Тайна», с обозначением сведений о ее владельце.

Статья 10 содержит данные об охране конфиденциальности сведений. Прописывает способы охраны коммерческой тайны, порядок установления режима коммерческой тайны, установление о том, что помимо способов защиты, прописанных в п.1 статьи, владелец может использовать механические способы сохранить тайну данных, и любые другие, не нарушающие законодательства страны.

Вероятный нарушитель информационной безопасности может быть: внешним, внутренним и комбинированным.

Внешний нарушитель – физическое лицо, не имеющее доступ на территорию предприятия, не сотрудничавшее с предприятием ранее, обладающее информацией о деятельности и структуре предприятия по данным, полученным из открытых источников.

Внутренний нарушитель – физическое лицо, имеющее доступ на территорию предприятия, либо сотрудничающее с предприятием, владеющее информацией о деятельности, структуре, политике информационной безопасности предприятия, полученной из открытых источников и внутренней документацией предприятия.

Комбинированный нарушитель – физическое лицо, ранее имевшее доступ на территорию предприятия, либо ранее сотрудничавшее с предприятием, обладающее информацией о деятельности, структуре, политике информационной безопасности предприятия, полученной из открытых источников и внутренней документацией предприятия.

Для каждого типа вероятного нарушителя существуют свои предположения об имеющейся у него информации:

1. Для внешнего нарушителя предполагается, что имеется вся информация, необходимая для подготовки и проведения атак, за исключением информации, доступ к которой со стороны нарушителя исключается системой защиты информации, а также за исключением сведений:
   * содержание технической документации на технические и программные компоненты средств физического контроля;
   * сведения о линиях связи, нарушениях правил эксплуатации крипто- средств и средств физического контроля;
   * сведения о неисправностях и сбои технических средств, криптосредств, средств физического контроля.

2. Для внутреннего предполагается, что нарушитель обладает информацией об объектах реализации угроз, их защищенности, о структуре предприятия, средствах защиты, топологии сети, организационном обеспечении информационной безопасности. Предполагается, что вероятный нарушитель имеет средства реализации угроз: аппаратные компоненты, криптосредства, технические средства и ПО, находящиеся в свободной продаже, которые возможно незаметно пронести, провезти на территорию предприятия через контрольно-пропускные пункты, либо замаскированные. Так же предполагается наличие информации о целях реализации угроз информационной безопасности;

3. Для комбинированного нарушителя предполагается, что он обладает информацией об объектах реализации угроз, их защищенности, о структуре предприятия, установленных средствах защиты, топологии сети, организационном обеспечении информационной безопасности. Предполагается, что вероятный нарушитель имеет средства реализации угроз, возможности которых не превосходят возможности аналогичных средств атак на информацию, содержащую конфиденциальные сведения.

Для составления модели угроз системы защиты, необходимо выявить объекты защиты. Объект защиты – информация, информационный процесс или устройство, которые необходимо защищать с целью сохранности информации. На основании анализа системы защиты коммерческой тайны предприятия составим перечень объектов, нуждающихся в защите:

1. Автоматизированные рабочие места сотрудников.
2. Линии и средства связи.
3. Работники предприятия.
4. Серверное оборудование и помещение.

Для данных объектов защиты был определен уровень исходной защищенности и были выявлены актуальные угрозы безопасности:

1. Угрозы утечки видовой информации.
2. Установка ПО, не связанного с исполнением служебных обязанностей.
3. Непреднамеренная модификация, уничтожение информации сотрудниками. Сбой системы электроснабжения.

5. Разглашение, модификация, уничтожение информации сотрудниками, допущенными к ее обработке.

Данные угрозы являются приоритетными для составления рекомендаций по модернизации системы защиты коммерческой тайны на предприятии, с целью устранения угроз информационной безопасности.

Ввод информации в информационную систему должен происходить путем занесения данных сотрудником на своем рабочем месте с использованием ПЭВМ и ЛВС через интерфейс пользователя на сервер баз данных, расположенный в ЦОДе.

Под обработкой информации понимается преобразование входной информации к формату, необходимому для ее хранения, преобразование хранимой информации к формату, соответствующему требованиям вывода информации на экран монитора, на печать с использованием принтера или МФУ, или передаче ее непосредственно на производственное оборудование. Обработка информации должна осуществляться сотрудниками подразделений, как в бумажном, так и в электронном виде с использованием ПЭВМ внутри своего подразделения. Пользователи ПЭВМ имеют разные права доступа к информации, хранящейся как на ПЭВМ, так и на сервере предприятия. Права доступа назначаются администратором безопасности сети штатными средствами серверной ОС и с использованием СЗИ от НСД Страж NT 3.0.

Вывод информации из системы осуществляется на мониторы ПЭВМ, принтера, МФУ и производственное оборудование, подключенное к ЛВС предприятия.

Передача информации в бумажном виде осуществляется собственноручно сотрудниками подразделений. Учет бумажных носителей осуществляется в журнале учета, табельщиком подразделения, в котором данный носитель был создан (напечатан). При производственной необходимости передачи копии данного носителя сотруднику другого подразделения, на оригинале ставится его подпись, после чего производственные операции выполняются по копии полностью подписанного носителя.

Для файлового обмена информацией в электронном виде между подразделениями предприятия служат каталоги, находящиеся на файловом сервере предприятия. Всем пользователям локальной вычислительной сети предприятия предоставляются полные права для каталога своего подразделения и права на запись для каталогов других подразделений. Сотрудник, забирающий предназначенную для него информацию из каталога своего подразделения, обязан перенести ее на свой компьютер для дальнейшей работы, удалив ее при этом из каталога.

Резервное копирование – процесс создания копии данных на носителе информации, предназначенном для восстановления данных в случае повреждения или разрушения оригинальной информации.

Резервное копирование происходит с периодичностью 1 раз в день. Восстанавливается утраченная информация путем ввода на ПЭВМ данных с сервера, записанных в последнюю сессию резервного копирования. Операции резервирования и восстановления фиксируются в электронном журнале. Бумажные носители восстанавливаются из существующих копий экземпляров или путем повторным распечатыванием утраченного документа.

В информационной системе предприятия реализовано плановое резервное копирование ключевых элементов информационной системы с сервера баз данных на выделенное дисковое хранилище с периодичностью 1 раз в день.

Для поддержания работоспособности системы в случае утраты/модификации информации рекомендуется:

* включить в план резервного копирования информацию с ПЭВМ руководителей подразделений;
* увеличить внутреннее пространство дискового хранилища, путем приобретения дополнительных жестких дисков.

Для анализа с целью расширения дискового пространства хранилища резервного копирования были выбраны три продукта категорий жестких дисков, представленных на рынке:

1. HGST Ultrastar HE12.
2. SEAGATE Ironwolf 12Тб.
3. WD Gold WD121KRYZ.

Как правило, предприятие подключено к электросети городского снабжения с трансформаторной подстанцией, размещенной в пределах контролируемой зоны предприятия. С целью ликвидации угрозы сбоя системы электроснабжения рекомендуется оборудовать ключевые элементы информационной системы источниками бесперебойного питания (ИБП). ИБП защищает технику от скачков напряжения и вызванных ими отказов оборудования, обеспечивает надежность и стабильность работы электроники.

По результатам анализа характеристик, перечисленных в таб. 2.1 был выбран жесткий диск HGST HUH721212ALE604.

Таблица 2.1 Оценка характеристик жестких дисков

|  |  |  |  |
| --- | --- | --- | --- |
| Устройство\  параметры | HGST Ultrastar HE12 | SEAGATE Ironwolf 12Тб | WD Gold WD121KRYZ |
| Средняя цена на рынке, руб. | 21810 | 25857 | 29500 |
| Наработка на отказ, ч. | 2500000 | 1000000 | 2500000 |
| Уровень шума при работе, дб | 36 | 32 | 36 |
| Уровень шума простоя, дб | 20 | 28 | 20 |
| Потребляемая мощность, вт | 7,2 | 7.8 | 6.9 |
| Гарантия производителя, мес. | 60 | 36 | 60 |
| Объем накопителя, тб | 12 | 12 | 12 |

Для анализа характеристик было выбрано три устройства из различных ценовых категорий, их сравнение приведено в таблице 2.2

Проанализировав все характеристики устройств, был выбран источник бесперебойного питания Ippon Back Comfo Pro 1000 New, ввиду его экономичности типа предохранителя, достаточной выходной мощности для обслуживания ключевого узла информационной системы и ценового превосходства относительно других.

Таблица 2.2 Характеристики источников бесперебойного питания

|  |  |  |  |
| --- | --- | --- | --- |
| Устройство\  Параметры | CyberPower  CP900EPFCLCD | CyberPower  CP1300EPFCLCD | Ippon Back Comfo  Pro 1000 New |
| Цена, руб. | 10243 | 13660 | 6850 |
| Выходная  мощность, Вт | 540 | 780 | 600 |
| Время работы при полной и половин-  ной нагрузке, мин | 1 и 7 | 2 и 9 | 3 и 30 |
| Максимальная  поглощаемая энергия импульса, Дж | 405 | 405 | 320 |
| Количество  разъемов питания | 6 | 6 | 8 |
| Отображение ин-  формации | ЖК-экран | ЖК-экран | Светодиодные  индикаторы |
| Тип предохрани-  теля | плавкий | плавкий | автоматический |

В информационной системе рекомендуется использовать различное программное обеспечение. Основное, распространенное ПО:

* различные версии ОС Windows;
* офисные пакеты Microsoft Office 2003-2007, LibreOffice 5.2;
* антивирусное Dr.Web 11.0 (сертификат ФСТЭК №3509 продлен до 27.01.2024);
* архивации 7Zip, WinRar;
* защиты информации DeviceLock 8 DLP Suite ,VipNet Client 4.
* профессиональные инструменты Компас-3D, Autodesk AutoCad.

Пользователями программно-аппаратного комплекса информационной системы предприятия являются сотрудники подразделений с разграничением прав к информационным ресурсам.

Схема информационных потоков предприятия подразумевает маршрут движения информации внутри информационной системы предприятия. ПЭВМ сотрудников подразделений имеют прямое подключение к принтерам и МФУ, находящимся в их подразделении и к локальной вычислительной сети предприятия.

При возникновении у работника производственной необходимости в получении информации из сети Интернет или использования электронной почты, он должен составить заявки на доступ к информационным ресурсам или передачу электронной почты, соответственно, в которых указывается пользователь, тип информационного ресурса, краткое содержание почтовых файлов, подпись начальника подразделения о проверке на отсутствие конфиденциальных сведений. Далее, информация, полученная из сети Интернет или электронной почты с помощью специального учтенного носителя информации, переносится на обособленное АРМ, с целью проверки и обработки информации. После проведения необходимых процедур, с помощью другого учтенного носителя информации полученные сведения заносятся администратором безопасности сети в каталог подразделения в личную папку работника, после чего он может осуществлять обработку информации со своего рабочего места.

При этом локальная вычислительная сеть (ЛВС) предприятия с размещенной в рамках нее информационной системой ограничена внутренним сегментом и не имеет физического подключения к внешней сети Интернет.

Дополнительно необходимо использовать следующие программные и аппаратные средства защиты:

* средство защиты информации от НСД «Страж NT» 3.0 (сертификат ФСТЭК №2145 до 30.07.2020);
* генератор пространственного зашумления «Соната Р2» (сертификат ФСТЭК №1129 до 16.01.2021);
* система виброакустической защиты «Соната-АВ» (модель 1М) (сертификат ФСТЭК №693 до 31.10.2020);
* блокиратор сотовой связи ЛГШ-701 (сертификат ФСТЭК №1252 до 05.09.2021).

Обобщенная схема информационных потоков представлена на рисунке 2.1

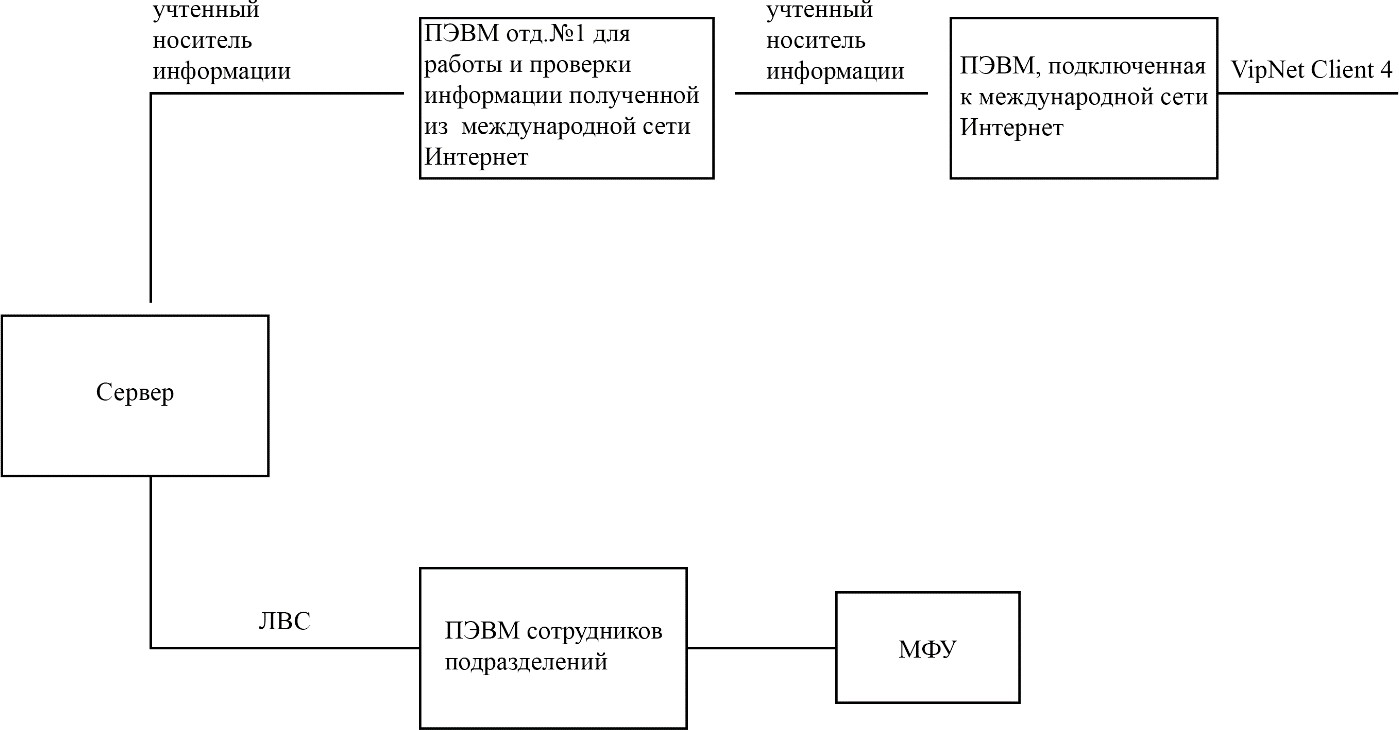


Рисунок 2.1 Обобщенная схема информационных потоков предприятия

Также рекомендуется установить антивирусную программу на все компьютеры на предприятии.

Главное предназначение антивирусной программы – это защита информации, которая хранится на компьютере от компьютерных вирусов.

Кроме защиты компьютера антивирус проверяет посещаемые Вами интернет-сайты и в случае обнаружения на сайте нежелательного ПО блокирует его. Так же антивирус убирает с большинства сайтов надоедливую рекламу.

Еще одна очень важная функция – это «Родительский контроль». Антивирус позволяет ставить запрет на посещение определенных сайтов.

Существует два основных пути заражения компьютера:

* скачивание, каких-либо зараженных файлов с Интернета.
* через съемные носители. Когда вирус уже присутствует на носителе и вовремя копирования информации он перемещается на компьютер.

Однозначного ответа какую антивирусную программу выбрать нет. Каждая программа имеет свои плюсы и минусы. Поэтому выбор остается только за конечным потребителем исходя из его предпочтений.

Какие функции должен иметь антивирус.

Набор обязательных функций, которые должны быть в наличии для корректной защиты компьютера.

* 1. Антивирусный мониторинг. Проверка папок и файлов, которые используются в данный момент на наличие вирусов.
  2. Сканер. Опция, которая позволяет проводить проверку жестких дисков компьютера на присутствие вирусов.
  3. Автозащита. Некоторые вирусы пытаются отключить работу антивируса, что бы этого не случилось, антивирус должен иметь автозащиту.
  4. Контроль работы программ. Если программа заражается вирусом, то процесс ее работы начинает меняться что и должен сразу обнаружить антивирус.
  5. Сетевой и интернет контроль. Важная функция, которая отвечает за работу компьютера в локальной сети или в Интернете.
  6. Обновление антивирусных баз. Учитывая то, что новые вирусы появляются чуть ли не каждый день, антивирус должен регулярно обновлять свою базу вирусов, чтобы максимально защитить компьютер.
  7. Ресурсопотребление. Лучше выбирать антивирусы с низким потреблением ресурсов компьютера. Чем данный показатель ниже, тем комфортнее работать за ПК.

Ниже приведено описание самых распространённых антивирусных программ. Антивирус Касперского.

Самый популярный российский антивирус. Имеет две вариации: Антивирус Касперского и Kaspersky Internet Security. Отличие между ними в том, что второй вариант помимо стандартной защиты ПК имеет еще и интернет-защиту что является важным плюсом.

Плюсы данной программы:

* высокая защита;
* множество дополнительных функций;
* широкие возможности настроек. Минусы программы:
* высокая стоимость лицензии;
* жесткий контроль процессов других программ.

Dr.Web. Антивирус занимает второе место по популярности и так же производится в России. Выпускается в двух версиях: простая и с интернет защитой. В сравнении с Антивирусом Касперского, Dr.Web немного проигрывает, как по количеству функции, так и по качеству защиты.

Avast Free Antivirus. Прекрасный бесплатный антивирус чешского производства. Имеет довольно хорошую защиту от вирусов как для бесплатного антивируса. Регулярно обновляет свою базу данных вирусов, что гарантирует максимальную защиту ПК.

NOD32. Производится в Словакии с 1987 года. Хороший антивирус главным преимуществом, которого есть малое потребление системных ресурсов компьютера. Существует так же расширенная версия антивируса NOD32 Smart Security, которая обеспечит надежную защиту компьютера при работе в интернете.

Каждый антивирус имеет как плюсы, так и минусы. Все зависит от предпочтений пользователя, имеющихся финансовых ресурсов, производительности компьютера. Нужно понимать, что нет антивируса с гарантированной стопроцентной защитой и возможность заразить компьютер остается всегда.

Таким образом, на основании анализа системы, составленной модели угроз и выявленных актуальных угроз информационной безопасности для предприятия был сформирован список рекомендаций для модернизации существующей системы защиты, также проведен анализ популярного антивирусного программного обеспечения с выявлением достоинств и недостатков по результатам тестов и личного опыта из открытых источников информации. Для защиты от актуальных угроз предложены меры:

* проведение дополнительных инструктажей по работе, ответственности и обновлению законодательства в сфере защиты информации и оснащение RFID считывателями серверного помещения;
* уменьшение категорий пользователей, с правами на установку стороннего программного обеспечения;
* увеличение элементов системы, для резервного копирования, а также увеличение дискового пространства хранилища резервных копий за счет жестких дисков типа HGST HUH721212ALE604;
* установка источников бесперебойного питания Ippon Back Comfo Pro 1000 New во все ключевые узлы системы.

На основании проведенного анализа обеспечения информационной безопасности и были выявлены проблемы, предложены рекомендации по разработке мероприятий по обеспечению сохранности коммерческой тайны. Часть необходимой документации была разработана, переработана и приложена к работе в приложениях.

# ЗАКЛЮЧЕНИЕ

Открытое использование информации, составляющей коммерческую тайну, угрожает экономической безопасности любого бизнеса, в связи с этим владелец бизнеса предпринимает меры по сохранению конфиденциальности этой информации и её защите от незаконного распространения и использования. Этот режим имеет четкую классификацию информации, подпадающей под коммерческую тайну.

Мероприятия предлагаемые по совершенствованию системы защиты коммерческой тайны могут казаться достаточно простыми и использованными не один раз на практике, но учитывая, что каждый «объект» несет за собой различные индивидуальные «нюансы», эти мероприятия, несомненно, повысят эффективность, как системы защиты коммерческой тайны, так и системы безопасности организации в целом.

Комплекс организационных мер, направленных на плановое обеспечение потребностей производства и предотвращение возможных инцидентов, способствует повышению эффективности обеспечения информационной безопасности. Нормативно-правовые документы и сотрудники контролирующих подразделений регулируют соблюдение норм и правил, описанных во внутренней распорядительной документации предприятия.

В настоящее время организационно-правовые, технические, программно-аппаратные, физические средства защиты информации являются неотъемлемой частью систем безопасности, которые как минимум, позволяют установить хронологию событий или предотвратить очередные действия злоумышленников. В организациях следует осознавать, что они являются местами повышенного внимания для «преступного мира». Привлекает злоумышленников разного рода информация или материальные ценности, если не говорить о различных попытках совершения терактов. Здесь же привычные мероприятия в организации поставят злоумышленников в трудное положение при попытке проникновении на объект, для осуществления каких-либо целей. Системы защиты ставят подобных преступников в неудобное положение, или вовсе исключают возможность проникнуть на объект незамеченным.

В ходе выполнения работы были решены следующие задачи:

* исследованы теоретические основы информационной безопасности;
* определено, что в организации в целях защиты коммерческой информации необходимо разработать ряд документов, регламентирующих деятельность по защите информации;
* предложены решения по устранению выявленных недостатков в системе защиты коммерческой тайны.

При внедрении предложенных мероприятий так же повышается уровень защищенности информационных, материальных и иных ценностей.

В результате выполнения выпускной квалификационной работы проведен анализ системы защиты информации, ознакомление с нормативно-правовой базой, составлен список рекомендаций по модернизации системы защиты коммерческой тайны и разработана необходимая документация для внедрения положений списка рекомендаций в систему защиты информации, составляющей коммерческую тайну предприятия.

Из всего вышеизложенного можно сделать вывод, что цель, обозначенная во введении данной работы, достигнута.

**СПИСОК ИСТОЧНИКОВ И ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ**

1. ИСТОЧНИКИ
2. Конституция РФ от 12 декабря 1993г.
3. «Доктрина информационной безопасности РФ», утв. Указом Президентом РФ 05.12 2016 г., № - 646.
4. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
5. Гражданский кодекс РФ от 30 октября 2002 г.
6. Федеральный закон от 29 июля 2004 г. N 98-ФЗ «О коммерческой тайне» с изменениями и дополнениями от 12 марта 2014 г.
7. Федеральный закон от 27 июля 2006 г. N 152-ФЗ «О персональных данных» с изменениями и дополнениями от 23 июля 2013 г. N 205-ФЗ.
8. Уголовный кодекс РФ от 5 июня 1996 г.
9. Государственная техническая комиссия при Президенте РФ. Сборник руководящих документов по защите информации от несанкционированного доступа. - М.: СИП РИА, 1997 г.

II. ЛИТЕРАТУРА

9. Алексенцев А.И. Понятие и структура угроз защищаемой информации // Безопасность информационных технологий [Текст].- 2000- № 3.- С. 79-84.

10. Алексеенко В.Н., Сокольский Б.В. Система защиты: Практическое пособие для предпринимателей и руководителей служб безопасности [Текст].- М., 1992- 280 с.

11. Алексеенко В.Н., Древс Ю.Г. Основы построения системы защиты производственных предприятий и банков [Текст]. - М.: МИФИ, 1996.- 268с.

12. Алексеенко В.Н., Саржин А.А. Организация проведения поисковых мероприятий. Специальная защита объектов: Пособие для сотрудников служб безопасности, руководителей деловых и коммерческих структур [Текст].- М.: Фирма «Росси Секьюрити», 1997.- 624с.

13. Бармен С. Разработка правил информационной безопасности [Текст]/ С.Бармен; Пер. с англ.- М.: Издательский Дом «Вильяме», 2002. - 208с

14. Волокитин А.В., Маношкин А.П., Солдатенков А.В., Савченко С.А., Петров Ю.А. Информационная безопасность государственных организаций и коммерческих фирм // Справочное пособие [Текст]. - М.: НТЦ «ФИОРД- ИНФО»,2002.- 846с.

15. Гаценко О.Ю. Защита информации. Основы организационного управления [Текст]: СПб, сентябрь 2001.- 298с.

16. Гавриш В. А. Практическое пособие по защите коммерческой тайны [Текст].- Симферополь: Таврия,1994.- 152с.

17. Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации [Текст]. – М.: Изд-во «Яхтсмен», 1996.-345 с.

18. Демик Н.К. Обеспечение безопасности информационных и телекоммуникационных систем // Методическое пособие [Текст].- М.: Рос. экон. акад.,2003.- 480 с.

19. Дорошенко П.С., Петраков А.В., Савлуков Н.В., Охрана и защита современного предприятия [Текст].- М.: Энергоатомиздат, 1999.-198 с.

20. Жуков В.Ф. Основы организации защиты информации [Текст]. – М.:Изд- во «ВиЛ»,2002.-334с.

21. Журавленко Н.И., Курбанов Д.А. Теория и методология защиты информации// Учебное пособие [Текст].- Уфа: Оперативная полиграфия, 2001.- 250с.

22. Кащеев В. И., Обеспечение информационной безопасности коммерческого объекта// Системы безопасности [Текст].- М.: Республика,1995.-334с.

23 Козлов С. Б., Иванов Е. В.,Предпринимательство и безопасность [Текст].-М.: Универсум,1991.- Т.1, 522с.

24 Корнеев И. К., Степанов Е. А., Защита информации в офисе//Учебник [Текст].- М.: Проспект,2007.- 333с.

25 Корт С.С. Теоретические основы защиты информации// Учебное пособие [Текст].- М.: Гелиос АРВ, 2004.- 240 с.

26 Куваев М. В., Чуфаровский Ю. В., Шиверский А. А., Коммерческая информация: способы получения и защиты [Текст]. – М.: Юрист,1996.-123с.

27 Мазеркин Д. Р., Защита коммерческой тайны на предприятиях различных форм собственности// Частный сыск и охрана [Текст]. – Саратов: Фараон, 1994.- 98с.

28 Минаев В.А., Скрыль С.В., Фисун А.П., Потанин В.Е., Дворякин С.В. Основы информационной безопасности // Учебник [Текст]. - Воронеж: Воронежский институт МВД России, 2000.- 400с.

29 Партыка Т.Д., Информационная безопасность// Учебное пособие для студентов среднего профобразования [Текст].- М.: ФОРУМ, ИНФРА,2004.- 368с.

30 Степанов Е.А., Корнеев И.К. Информационная безопасность и защита информации // Учебное пособие [Текст].- М.: ИНФРА, 2001.- 418с.

31 Торокин А.А. Инженерно – техническая защита информации [Текст].- М.: Изд- во «Гелиос АРВ», 2005.- 960с.

32 Филин С.А. Информационная безопасность [Текст].- М.: Изд- во «Альфа- Пресс», 2006.- 412с.

33. Шиверский А. А., Защита информации: проблемы теории и практики. [Текст]. - М.: Юрист, 1996.- 119с.

34. Ярочкин В. И. Информационная безопасность// Учебник для вузов [Текст].- М.: Изд- во «Академический Проект», 2006.-543с.

III. ЭЛЕКТРОННЫЕ РЕСУРСЫ

35. <https://ru.wikipedia.org> (дата обращения 20.04.2020).

36. <http://www.garant.ru> (дата обращения 26.04.2020).

37. <https://www.polyvision.ru> (дата обращения 20.05.2020).

38. <http://texno-proekt.ru> (дата обращения 23.05.2020).