**Федеральное агентство связи**

**Ордена Трудового Красного Знамени**

**федеральное государственное бюджетное образовательное учреждение высшего образования**

**«Московский технический университет связи и информатики»**

**Кафедра «Информатика»**

**Курсовая работа по дисциплине «Основы программирования»**

**на тему**

**«Менеджмент в сфере информационной безопасности»**

Выполнила студентка группы БСТ2002

Иванова М.С.

Проверил: доц. Гуриков С. Р.

**СОДЕРЖАНИЕ**

[**ВВЕДЕНИЕ** 4](#_Toc54872149)

[**ТЕХНИЧЕСКОЕ ЗАДАНИЕ** 7](#_Toc54872150)

[**ГЛАВА 1** 9](#_Toc54872151)

[**1.1 Основные направления развития менеджмента в сфере информационной безопасности** 9](#_Toc54872152)

[**1.2 Деятельность международных организаций в сфере информационной безопасности** 14](#_Toc54872153)

[**1.3 Деятельность специализированных международных организаций и объединений в сфере информационной безопасности** 16](#_Toc54872154)

[**1.4 Альянсы крупных технологических компаний** 16](#_Toc54872155)

[**1.5 Управление информационной безопасностью на уровне крупных поставщиков информационных систем** 17](#_Toc54872156)

[**1.6 Управление информационной безопасностью на государственном уровне** 19](#_Toc54872157)

[**1.7 Менеджмент информационной безопасности на уровне предприятия: основные направления и структура политики безопасности** 20](#_Toc54872158)

[**1.7.1 Формирование политики информационной безопасности на предприятии** 21](#_Toc54872159)

[**1.8 Содержание детализированной политики безопасности** 21](#_Toc54872160)

[**1.9 Департамент информационной безопасности и работа с персоналом** 22](#_Toc54872161)

[**1.9.1 Организационная структура и персонал департамента информационной безопасности** 23](#_Toc54872162)

[**1.9.2 Работа с персоналом предприятия** 24](#_Toc54872163)

[**1.10 Организация реагирования на чрезвычайные ситуации (инциденты)** 24](#_Toc54872164)

[**1.11 Аудит состояния информационной безопасности на предприятии** 25](#_Toc54872165)

[**1.12 Программные средства, поддерживающие управление информационной безопасностью на предприятии** 26](#_Toc54872166)

[**1.12.1 Программная поддержка работы с политикой безопасности** 27](#_Toc54872167)

[**1.12.2 Программная поддержка анализа рисков** 27](#_Toc54872168)

[**1.12.3 Программные средства, интегрируемые в информационную систему предприятия** 28](#_Toc54872169)

[**1.13 Предоставление услуг в сфере информационной безопасности** 28](#_Toc54872170)

[**1.13.1 Страхование информационных рисков. Основы методологии страхования информационных ресурсов** 29](#_Toc54872171)

[**1.14 Экономика информационной безопасности** 30](#_Toc54872172)

**ОЧЕНЬ МНОГО ПУНКТОВ. ВАС ОРИЕНТИРОВАЛИ НА 1.1 – 1.3**

# **ВВЕДЕНИЕ**

**Актуальность темы**. Нынешняя практика использования информационных систем характеризуется огромным количеством и постоянным увеличением нарушений информационной безопасности. Важным фактором для этого является повышение доступности современных информационных технологий для преступников, а также повышение привлекательности информационных систем как потенциальных объектов нападения. И не менее значимым фактором является постоянное усложнение и рост разнообразия используемых информационных систем и, в частности, программных продуктов. Как результат мы имеем непрерывное увеличение количества нарушений, связанных с информационной безопасностью.

**Из вышесказанного следует**, что современное общество, а именно владельцы информационных ресурсов (предприятий, организаций, государственных ведомств) нуждаются в реализации систематических, комплексных мер по обеспечению информационной безопасности, что подтверждает актуальность проблемы.

Во всех областях информационной безопасности одним из важнейших мест занимает организационная и управленческая деятельность - организационное обеспечение информационной безопасности, которое включает в себя разработку специализированного программного обеспечения, изготовление и использование специальных аппаратных средств и совершенствование криптографических (математических) методов защиты информации.

Управление человеческими ресурсами в рамках управления информационной безопасностью включает в себя задачи, охватывающие все основные аспекты работы людей: подбор и допуск сотрудников к работе с определенными информационными ресурсами, обучение, контроль за правильным выполнением задач, создание необходимых условий труда и т.п.

**Наряду с этим** структура и состав всех основных задач регулирования и организации в области информационной безопасности, включая непосредственно используемые методы, определяются как уровнем, на котором осуществляется управленческая и организационная деятельности, так и конкретными условиями, при которых функционирующие информационные системы нуждаются в защитной функции.

Дополнительным подтверждением актуальности темы является потребность глобализации информационных взаимодействий в более полном и широком понимании организационной работы и менеджмента в области информационной безопасности.

**Можно сказать**, что в условиях глобализации информационных взаимодействий, усложнения и усовершенствования программных и аппаратных условий обработки информации, проникновения информационных технологий в повседневную деятельность всех организаций и жизнь многих людей появилась потребность в особых организационных и управленческих усилий, направленных не на обеспечение безопасности оборудования для отдельных информационных активов, а на поддержание различных элементов инфраструктуры, которые обеспечивают безопасность определенных сообществ.

**Объектом исследования** является информационная безопасность.

**Предметом исследования** является менеджмент в сфере информационной безопасности.

**Цели работы и задачи исследования.** Цель работы – исследование способов управления, принципов и организации работы в сфере информационной безопасности и разработать программу для изучения данной темы. Поставленная цель определила следующие задачи исследования:

1. Проанализировать теоретический материал.
2. Разработать программу, в которой будет находиться теоретический материал по теме и тестирование на ее знание.

**Методы исследования.** Для решения поставленных задач были использованы теоретические методы исследования. Теоретическую основу исследования написал Анисимов А.А.

# **ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

**1.1 Основание для разработки**

Основанием для разработки является задание, выполненное в соответствии с заданием, полученным от кафедры «Информатика» Московского технического университета связи и информатики и утвержденным научным руководителем доцентом кафедры «Информатика» К.П.Н. Гуриковым С.Р. 2 октября 2020 года.

**1.2 Назначение разработки**

Программный продукт предназначен для ознакомления с основными теоретическими положениями по теме курсовой работы и проверки знаний пользователя с помощью тестовой программы.

**1.3 Требования к программному изделию**

**1.3.1 Требование к функциональным характеристикам**

Разработанный программный продукт должен обеспечить выполнение следующих функций:

- возможность ознакомления с теоретическим материалом по теме курсовой работы,

- возможность вывода результатов исследования для пользователя.

**1.3.2 Требования к надежности**

Разрабатываемое программное обеспечение должно иметь:

- устойчивую работу, в соответствии с алгоритмом программы,

- выдавать сообщения об ошибках,

-\\поддерживать диалоговый режим в рамках предоставляемых пользователю возможностей,

**1.3.3 Требование к составу и параметрам технических средств**

- Минимальные системные требования

-Рекомендованные системные требования

И ГДЕ ЖЕ ОНИ ПЕРЕЧИСЛЕНЫ??

**1.3.4 Требование к информационной программной совместимости**

Программа должна легко инсталлироваться и функционировать при наличии следующего программного обеспечения:

**1.3.5 Требование к транспортированию и хранению**

Программная документация поставляется в электронном и печатном виде.

**1.3.6 Требование к программной документации**

В ходе разработки программы должны быть подготовлены: текст, программный текст, описание, методика испытаний, руководство пользователя.

**1.3.7 Стадии и этапы разработки**

Таблица 1 – Стадии и этапы разработки

|  |  |  |  |
| --- | --- | --- | --- |
| Номер этапа | Название этапа | Срок выполнения | Отчет |
| 1 | Утверждение темы | До 02.10.2020 | Выбранная тема была утверждена научным руководителем |
| 2 | Написание введение | До 15.10.2020 | Введение было утверждено научным руководителем |
| 3 | Написание технического задания и главы 1 | До 29.10.2020 |  |

# **ГЛАВА 1 НАЗВАНИЕ??**

## **1.1 Основные направления развития менеджмента в сфере информационной безопасности**

Решение задачи информационной безопасности не состоит только из технических средств. Во всем комплексе деятельности по защите информации одно из наиболее важных мест занимает менеджмент – организационное обеспечение информационной безопасности, которое представляет собой одно из четырех основных направлений работы в общей системе мер в сфере информационной безопасности, которая, помимо этого, включает в себя разработку специализированного программного обеспечения, изготовление и использование специальных аппаратных средств и совершенствование криптографических (математических) методов защиты информации.

Криптография и математика

Программное обеспечение

Аппаратное обеспечение

Организационное обеспечение (менеджмент)

Информационная безопасность

***Рисунок 1 – Структура деятельности в сфере информационной безопасности***

Основными задачами организационно-управленческой деятельности(менеджмента) в сфере информационной безопасности являются:

- обеспечение комплексности всех решений, реализуемых в процессе обеспечения информационной безопасности (взаимоувязанное выявление всех значимых информационных объектов, а также существующих и потенциально возможных угроз);

- обеспечение беспрерывность, целостность процессов информационной безопасности (выделение требуемых ресурсов и организацию выполнения необходимых функций по защите информации в течение всего, включая ситуации, где это нужно круглые сутки);

- решение методических задач, лежащих в основе эффективного управления информационной безопасностью, таких, как вопросы управления рисками, экономическое моделирование и т.п. (рассмотрение теорий, построение математических моделей для оценки рисков и пр.);

- управление человеческими ресурсами и поведением персонала с учетом необходимости решения задач информационной безопасности (контроль над правильностью выполнения заданий, обучение персонала, его отбор и обеспечение его конкретными информационными ресурсами).

**Из выше сказанного можно сказать**, что менеджмент в сфере информационной безопасности направлен как на защиту определенных информационных ресурсов, так и на более масштабное– составление и усовершенствование безопасной информационной инфраструктуры. На практике данная инфраструктура может содержать:

* безопасную инфраструктуру передачи информации и рынок услуг доступа к таким каналам связи;
* систему обмена информацией и распространения знаний о существующих уязвимостях тех или иных информационных технологий, возможных угрозах информационной безопасности и способах их устранения;
* рынок программных и аппаратных средств, которые обеспечивают защиту информации;
* общие правила использования, передачи информации;
* систему подготовки, переподготовки и повышения квалификации специалистов в области информационной безопасности;
* и прочие составляющие.

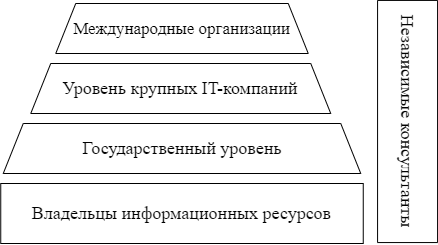
Необходимость развития и целенаправленного поддержания такой инфраструктуры возникает потребность в разработке конкретных организационных и управленческих методов, которые обычно не характерны для информационной безопасности в узком смысле.

**Таким образом**, принято разделять на несколько самостоятельных уровней, которые организованны и характеризуются разными специфическими задачами, подходами к той или иной задачей.

* Уровень международных профессиональных объединений, которые как-то связаны со сферой информационных технологий, телекоммуникаций и их безопасности.
* Уровень крупных компаний, работающих в области информационных технологий, во многом определяет (прямо или косвенно) безопасность информации в обществе пользователей информационных систем, а также безопасность различных элементов информационной инфраструктуры.
* Государственный уровень (где государственные и межправительственные организации, влияют на развитие экономики и технологий, жизнь социума и на правовую систему).
* Уровень отдельных компании (организаций и предприятий)- это сообщество пользователей, непосредственно заинтересованных в обеспечении собственной информационной безопасности и защите имеющихся у них информационных ресурсов собственными силами.

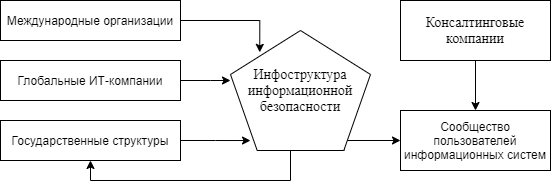
Также отдельно можно выделить промежуточный уровень, в том числе консалтинговые и внедряющие компании, учебные центры, которые выступают в качестве связующего звена между различными уровнями организации и представляют интересы разных участников информационного взаимодействия.

Все они составляют следующую иерархию (Рисунок 2):



**Рисунок 2 - Иерархия уровней организационной работы**

Представленное разделение на уровни является основой для более целенаправленного развития системы менеджмента и налаживания взаимосвязей между различными уровнями организационной работы, что указаны на рисунке 3.



**Рисунок 3 - Взаимосвязи уровней организации информационной безопасности**

Основные особенности организационной работы на каждом из перечисленных уровней организации представлены в Таблице 1.

**Таблица 2 - Задачи, роли и методы, используемые на различных уровнях организационной работы в сфере информационной безопасности**

|  |  |  |
| --- | --- | --- |
| Организационный уровень | Основные задачи и роли | Основные специфичные методы организационной работы |

**Продолжение таблицы 2**

|  |  |  |
| --- | --- | --- |
| 1.Международные организации | Разработка правил и стандартов (в том числе и сетевых протоколов),имеющих глобальное значение.  Обмен актуальной информацией и предупреждениями о новых угрозах | Координация работы специалистов, экспертов и исследователей, представляющих различные заинтересованные стороны |
| 2. Глобальные ИТ-компании | Методологическая и организационная поддержка использования продуктов и услуг, поставляемых на рынок | Гибкое взаимодействие с клиентами (пользователями продуктов и услуг) с целью повышения эффективности использования информационных систем и получения отзывов для дальнейшего повышения качества поставляемых продуктов и услуг |
| 3.Государственные организации | Регулирование использования информационных систем и распространения информации с целью недопущения противоправных действий, ущерба другим участникам информационного обмена, обществу и государственным органам | Разработка национальных и международных правил (законов, конвенций, соглашений и т.п.), регулирующих отношения в информационной сфере Осуществление контроля (в различных формах)  Осуществление правоприменительной и правоохранительной деятельности |
| 4. Пользователи информационных систем – владельцы информации | Защита собственных информационных ресурсов | Выделение подразделений и специалистов, отвечающих за ИБ |

**Продолжение таблицы 2**

|  |  |  |
| --- | --- | --- |
|  |  | Разработка и применение внутренних политик и правил безопасности |
| 5.Консалтинговые и консалтинговые и внедренческие компании, работающие в сфере ИБ | Выполнение некоторых функций ИБ на условиях аутсорсинга  Разработка и внедрение индивидуальных решений в сфере ИБ более эффективно, чем это могли бы сделать сами владельцы информационных ресурсов | Накопление и обобщение теоретических знаний и практических навыков с практических навыков с целью создания и внедрения организационных и технических решений в интересах клиентов |

Таблица 2 и рисунок 3 еще раз указывают на причины, по которым разный из уровней требует своего собственного подхода и применении специфических методов организационной работы и управления.

## **1.2 Деятельность международных организаций в сфере информационной безопасности**

В числе международных организаций находятся:

* Крупные международные некоммерческие и неправительственные организации, объединяющие специалистов в определенных областях, которые обычно существуют уже много лет и охватывают многие основные направления развития вычислительной техники, электроники и телекоммуникаций, включая определенные вопросы безопасности современных информационных технологий.
* Относительно небольшие отдельные организации (на базе частных компаний или исследовательских структур), которые в последнее десятилетие более или менее вовлечены в вопросы информационной безопасности, имеющие огромное значение во всем мире в сообществе пользователей информационных систем.
* Совместные структуры (комитеты, альянсы и т.п.), создаваемые (иногда временно) крупными компаниями (иногда при участии крупных исследовательских центров, учебных заведений и правительственных структур) для решения определенных задач в сфере информационных технологий и информационной безопасности.

Каждые, **из выше перечисленных**, имеют свои организационные особенности, однако решают задачи разработки, согласования и дальнейшего распространения общих для всего сообщества пользователей информационных систем технических и организационных решений (протоколы глобальных сетей; архитектуры, алгоритмы, протоколы публичных средств шифрования данных).

**Нельзя не отметить** важные элементы организационной работы на уровне международных структур:

* организация обмена знаниями и актуальными новостями в среде специалистов по информационной безопасности в таких формах, как публикация специализированных периодических изданий и сборников научных работ, организация специализированных научно-практических конференций, семинаров и т.п.;
* организация и поддержание в актуальном состоянии баз данных и баз знаний, которые содержат сведения, необходимые пользователям информационных систем, администраторам, разработчикам и другим участникам для обеспечения информационной безопасности.

Организационные принципы, характерные для многих международных организаций:

* Принцип добровольности участия в работе таких структур и вот дельных проектах или во всей работе.
* Принцип открытости (доступности) результатов работы (всех или их части) для сообщества специалистов в сфере информационных технологий.
* Принцип самофинансирования.

## **1.3 Деятельность специализированных международных организаций и объединений в сфере информационной безопасности**

Специализированные организации, оказывающие глобальное влияние на управление информационной безопасностью на различных уровнях и общее состояние информационной безопасности, могут выполнять функции мониторинга на базе:

* частных компаний, занимающихся исследованиями, разработками и консультированием в сфере информационной безопасности;
* крупных учебных заведений, специализирующихся на информационных технологиях, а также обладающих существенным авторитетом и финансовыми ресурсами;
* правительственных учреждений, ответственных за обеспечение информационной безопасности в определенных сферах.

Основным направлением организационной работы, проводимой в таком виде, является формирование и поддержание баз данных, содержащих информацию об известных уязвимостях различных программных и аппаратных средств, а также других форм информационной, консультативной и методической работы в этой области. Важными факторами успешного функционирования таких организаций являются интеграция информации из как можно большего количества источников и наиболее эффективное распространение информации в сообществе пользователей информационной системы.

**1.4 Альянсы крупных технологических компаний**

Высокая значимость формы организационной работы в области информационной безопасности, как формирование альянсов крупных и средних предприятий, специализирующихся на информационных технологиях, обусловлена тем, что:

* такие альянсы способны осуществить наиболее крупные инвестиции в разработку новых технологий и проведение исследований, которые могут повлиять на все развитие информационных технологий и состояние дел в сфере информационной безопасности;
* компании, входящие в такие альянсы, занимают значительную долю рынка и потому определяют общее направление развития информационных технологий вообще и средств защиты информации в частности;
* такие альянсы компаний способны создать комплексные технологии, продукты и решения, охватывающие различные аспекты функционирования информационных систем и средств защиты информации, и таким образом достичь нового уровня защищенности информации.

Задачами формирования альянсов могут быть:

* разработка новых продуктов и услуг, а также базовых технологий, протоколов, алгоритмов и соглашений, на основе которых такие продукты и услуги в будущем могли бы разрабатываться;
* формирование новых рынков сбыта и поддержка существующих;
* влияние на государственные и общественные организации, а также на сообщество пользователей информационных систем с целью обеспечения развития и более широкого использования информационных технологий и средств информационной безопасности;
* влияние на систему профессиональной подготовки специалистов с целью обеспечения качества их обучения.

**1.5 Управление информационной безопасностью на уровне крупных поставщиков информационных систем**

Основные приемы и методы внешней организационной работы в сфере информационной безопасности на уровне крупных компаний–поставщиков информационных систем могут быть следующие:

* организация информационного обмена с пользователями выпускаемых продуктов – программных и аппаратных средств (информирование о выявленных уязвимостях и способах их устранения, получение информации об уязвимостях, выявленных пользователями, а также других возникающих проблемах);
* организация деятельности в сфере подготовки специалистов (система подготовки квалифицированного инженерно-технического персонала, специализирующегося на определенных программных продуктах и, в частности, на администрировании средств защиты информации, сетевых операционных систем и т.п.);
* организация профессиональных конференций, которые способствуют обмену опытом и информацией, связанной с повышением уровня информационной безопасности при использовании определенных программных и аппаратных платформ;
* организация взаимодействия с правительственными организациями (в том числе по вопросам сертификации программных и аппаратных средств на соответствие требованиям национальных стандартов и правил);
* создание и поддержание системы сертификации специалистов, ориентированной на определенные программные продукты и аппаратные системы (в том числе, организация взаимодействия со специализированными компаниями, занимающимися профессиональным тестированием специалистов и др.).

## **1.6 Управление информационной безопасностью на государственном уровне**

Организационная деятельность государства в сфере информационной безопасности сводится к противодействию различным угрозам:

* внешним (например, деятельность иностранных спецслужб и вооруженных сил, агрессивная рыночная стратегия крупных международных корпораций и финансово-промышленных групп, незаконная деятельность международных преступных и террористических группировок и т.п.);
* внутренним (например, неправомерные действия государственных структур, халатность или целенаправленные нарушения, допускаемые гражданами и организациями при использовании информационных систем, нарушения в работе информационных и телекоммуникационных систем и т.п.).

Для обеспечения информационной безопасности государство делает следующее:

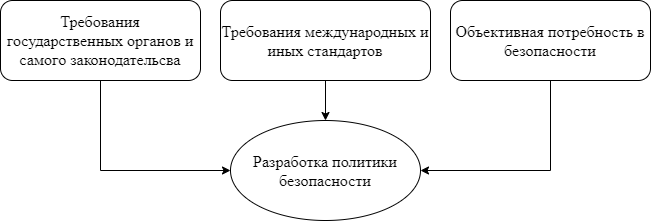
* создают законодательную базу, обеспечивающую защиту базовых прав частных лиц, предприятий и государства;
* осуществляют правомерную деятельность, выполняют все функции для реализации требования законодательства;
* выполняют судебные функции в отношении лиц, совершивших правомерное действие.

**Таким образом**, на практике деятельность органов власти, **как правило**, концентрируется на решении вопросов информационной безопасности внутри отдельных сфер, которые считаются наиболее важными для обеспечения государственной безопасности и достижения политических целей (вооруженные силы, внешняя разведка, стратегические технологии и пр.).

## **1.7 Менеджмент информационной безопасности на уровне предприятия: основные направления и структура политики безопасности**

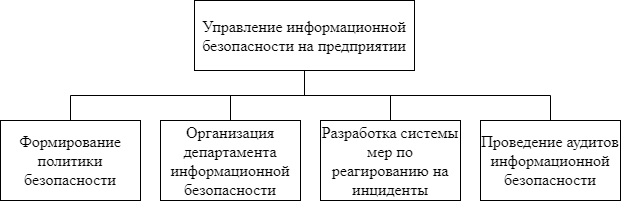
Управление информационной безопасностью на каждом предприятии должно осуществляться, отталкиваясь от его общей хозяйственной деятельности: с учетом характера деятельности компании(технологии производства, специфики рынков сбыта и т.п.), а также фактически складывающейся ситуации в рыночной конкурентной борьбе, государственной политике, развития правовой и правоохранительной системы, уровня развития отдельных используемых информационных и телекоммуникационных технологий и других факторов, формирующих общие условия текущей деятельности.

**Таким образом**, выше сказанное дает нам предпосылки менеджмента в информационной безопасности на уровне предприятий (Рисунок 4):



**Рисунок 4 - Предпосылки разработки политики безопасности предприятия**

Для нейтрализации существующих угроз и обеспечения информационной безопасности предприятия организуют систему менеджмента в сфере информационной безопасности, в рамках которой (системы) проводят работу по нескольким направлениям (Рисунок 5):



**Рисунок 5 - Структура организационной деятельности в сфере информационной безопасности на предприятии**

### **1.7.1 Формирование политики информационной безопасности на предприятии**

Разработка политики безопасности предполагает осуществление ряда предварительных шагов:

* оценку личного (субъективного) отношения к рискам предприятия его собственников и менеджеров, ответственных за функционирование и результативность работы предприятия в целом или отдельные направления его деятельности;
* анализ потенциально уязвимых информационных объектов;
* выявление угроз для значимых информационных объектов\ и оценку соответствующих рисков.

## **1.8 Содержание детализированной политики безопасности**

Основной задачей обеспечения внутри объектового режима является недопущение посторонних лиц к информационным активам и предотвращение угроз информационной безопасности. Основой внутриобъектового режима является пропускной режим, в рамках которого, **как правило**, устанавливаются:

* документы, дающие право прохода на территорию предприятия –как пропуска и карты доступа, выданные самим предприятием, так и документы, выданные сторонними организациями(например, служебные удостоверения должностных лиц некоторых органов государственной власти);
* категории пропусков, используемых на предприятии, в соответствии с которыми (категориями) ограничивается срок действия пропусков, время возможного прохода на территорию предприятия (дни недели, часы суток) и некоторые другие параметры;
* порядок выдачи, обмена, продления и изъятия пропусков, а также порядок действий сотрудников и должностных лиц при утрате пропуска;
* порядок организации пропуска лиц, автотранспорта и проноса(провоза) имущества;
* основные положения документооборота, используемого при проходе посетителей на территорию предприятия — требования к ведению Журнала регистрации прохода посетителей, требования к документам, на основе которых выдаются разовые пропуска, порядок выдачи разовых пропусков и т.п.;
* порядок досмотра транспортных средств, допускаемых на территорию предприятия.

## **1.9 Департамент информационной безопасности и работа с персоналом**

Департамент информационной безопасности (далее – департамент)предприятия представляет собой самостоятельное структурное подразделение предприятия, непосредственно выполняющее ключевые функции защиты информационных ресурсов.

**Как правило**, заключается в следующих аспектах:

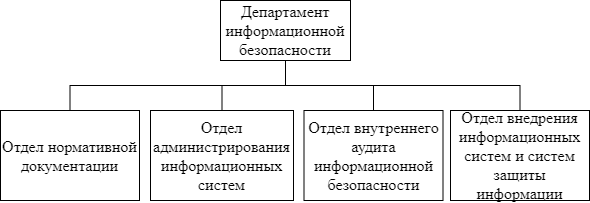
* организация и координация работ по обеспечению комплексной защиты информации на предприятии;
* контроль за выполнением требований и оценка эффективности работы подразделений и персонала предприятия по обеспечению информационной безопасности;
* выполнение отдельных административных и технических функций по обеспечению информационной безопасности (а именно внедрение различных).

**Из выше сказанного следует**, что состав задач департамента и его внутренняя организационная структура в каждом конкретном случае определяется такими особенностями функционирования предприятия, как:

* значимость информационных ресурсов в работе предприятия и характер существующих угроз;
* отношение руководства и собственников предприятия к вопросам информационной безопасности и их управленческая квалификация;
* функциональность и характер используемых информационных систем, их роль в бизнес-процессах;
* организация работы и структура ИТ-службы;
* финансовое состояние предприятия.

### **1.9.1 Организационная структура и персонал департамента информационной безопасности**

В составе департамента для повышения эффективности работы могут быть выделены самостоятельные группы (отделы), специализирующиеся на выполнении определенных функций (Рисунок 6):



**Рисунок 6 - Пример организационной схемы Департамента информационной безопасности предприятия**

### **1.9.2 Работа с персоналом предприятия**

Цели работы с персоналом предприятия:  
отбор и предварительная проверка персонала, принимаемого на работу (на службу);

* обучение сотрудников;
* достижение взаимопонимания руководителей и сотрудников в вопросах обеспечения информационной безопасности;
* психологическая подготовка с целью противостояния методам т.н. "социальной инженерии".

## **1.10 Организация реагирования на чрезвычайные ситуации (инциденты)**

Процесс реагирования на такого рода инциденты включает в себя четыре основных этапа:

1. обнаружение нападения;

2. локализация нападения;

3. идентификация нападающих;

4. оценка и последующий анализ процесса нападения и его обстоятельств.

В общем случае организационные процедуры (регламенты) реагирования на чрезвычайные ситуации должны включать в себя:

* регламенты альтернативных процессов обработки информации (в том числе, возможно, и без использования средств автоматизации) на период выхода из строя основных информационных ресурсов;
* определение групп персонала, ответственных за выполнение тех или иных функций в случае возникновения чрезвычайной ситуации, а также определение процедур взаимодействия между группами и отдельных групп с руководством предприятия;
* техническую и организационную документацию, необходимую для восстановления информационных систем и данных после чрезвычайной ситуации;
* порядок хранения архивных (резервных) копий данных и программных приложений обработки данных в местах, защищенных от механических воздействий, краж, наводнений, пожаров и т.п. (в т.ч., возможно, в местах, территориально удаленных от основных мест хранения и обработки информации);
* соглашения с поставщиками программных и аппаратных средств, входящих в информационную инфраструктуру предприятия, о срочной поставке компонент, вышедших из строя и требующих замены в случае чрезвычайной ситуации.

## **1.11 Аудит состояния информационной безопасности на предприятии**

Различают два основных вида аудита: внутренний (проводимый исключительно силами сотрудников предприятия) и внешний(осуществляемый сторонними организациями).

Целями аудита могут быть:

* установление степени защищенности информационных ресурсов предприятия, выявление недостатков и определение направлений дальнейшего развития системы защиты информации;
* проверка руководством предприятия и другими заинтересованными лицами достижения поставленных целей в сфере информационной безопасности, выполнения требований политики безопасности;
* контроль эффективности вложений в приобретение средств защиты информации и реализацию мероприятий по обеспечению информационной безопасности;
* сертификация на соответствие общепризнанным нормам и требованиям в сфере информационной безопасности (в частности, на соответствие национальным и международным стандартам).

Основными этапами проведения аудита являются:

* инициирование проведения аудита;
* непосредственно осуществление сбора информации и проведение обследования аудиторами;
* анализ собранных данных и выработка рекомендаций;
* подготовка аудиторского отчета и аттестационного заключения.

## **1.12 Программные средства, поддерживающие управление информационной безопасностью на предприятии**

Выделяется отдельный класс специальных программных продуктов, предназначенных исключительно для поддержания процессов разработки политик безопасности и управления информационной безопасностью на организационном уровне. Основными функциями таких программ являются справочно-информационная поддержка, помощь при обработке управленческой информации, оценке рисков и подготовке необходимых документов. В частности, для этих целей может использоваться ПО следующих основных видов:

* сборники (интерактивные электронные справочники), которые содержат типовые документы (шаблоны документов),используемые для управления информационной безопасностью, описания отдельных процессов и процедур, связанных с обеспечением информационной безопасности, должностных обязанностей и функций сотрудников предприятия;
* системы, предназначенные для накопления и обработки сведений о рисках и проведения сводных оценочных расчетов показателей риска;
* ПО, интегрированное в информационную систему предприятия и позволяющее автоматически контролировать соблюдение установленных политик безопасности, а также помогающее формировать заключения о текущем состоянии информационной безопасности (в т.ч. путем анализа действий пользователей в информационной системе, а также путем анализа журналов операционных систем, программ, средств защиты и сетевого оборудования);
* ПО, осуществляющее поддержку процессов аудита информационной безопасности.

### **1.12.1 Программная поддержка работы с политикой безопасности**

Сборники (справочники), которые содержат типовые документы, связанные с обеспечением информационной безопасности, могут включать в себя:

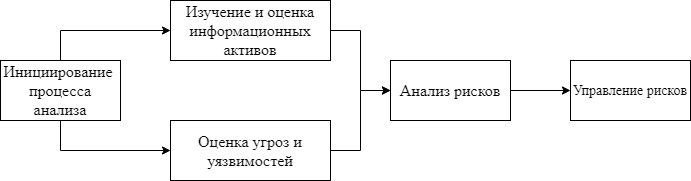
* образцы политик безопасности разных уровней для предприятий, функционирующих в различных сферах деятельности и предъявляющих различные требования к уровню защищенности информации;
* образцы (шаблоны, бланки) документов, используемых в процессах защиты информации (обязательств о неразглашении информации, отчетов о состоянии информационной безопасности и т.п.);
* образцы разделов различных договоров (контрактов с различными контрагентами или трудовых договоров с сотрудниками предприятия), содержащие требования к обеспечению информационной безопасности.

### **1.12.2 Программная поддержка анализа рисков**

Методологии анализа рисков и программные средства, реализующие эти методологии, как правило, предполагают выполнение следующих основных шагов, необходимых для формирования комплексной оценки существующих рисков:

* сбор информации об объектах защиты;
* выявление и оценка возможных угроз и уязвимостей;
* формирование сводной оценки рисков.

Выявлены следующие принципы работы (Рисунок 7):



**Рисунок 7 - Общая схема принципов работы**

### **1.12.3 Программные средства, интегрируемые в информационную систему предприятия**

Основные функции таких программных средств:

* проверка действий пользователей на их соответствие действующим политикам безопасности;
* выявление нарушений действующей политики информационной безопасности;
* установление лиц, чьи действия приводят к нарушениям и создают угрозы информационной безопасности.

## **1.13 Предоставление услуг в сфере информационной безопасности**

Каждый вид услуг в этой сфере имеет свои специфические характеристики как с точки зрения организации работы компаний, оказывающих услуги, так и с точки зрения структуры рынка. Соответственно, для эффективной работы необходим индивидуальный подход к организации оказания таких услуг, а также организации взаимодействия между потребителями и поставщиками услуг. Такая деятельность имеет следующие важные особенности:

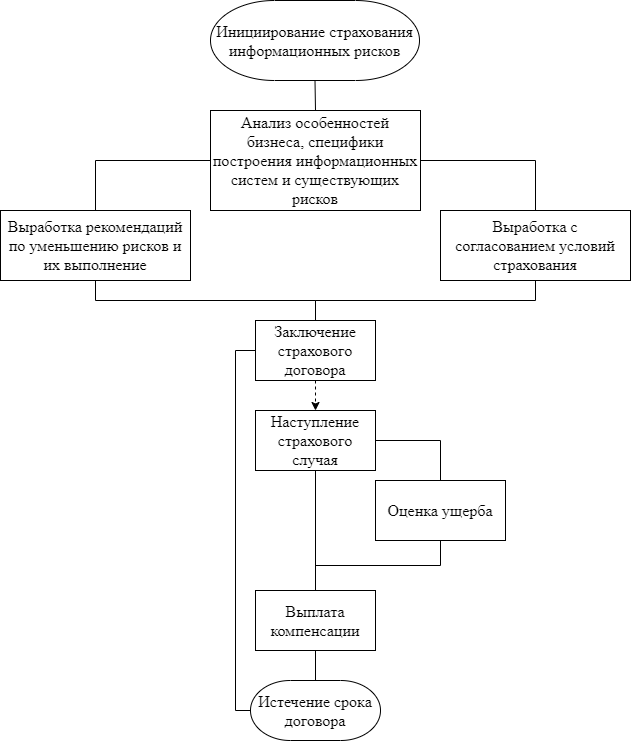
* требует постоянного (круглосуточного) дежурства, что предполагает содержание в штате как минимум пяти специалистов;
* предполагает наличие высококвалифицированных (а следовательно, высокооплачиваемых и востребованных на рынке труда) специалистов, способных быстро предпринять эффективные меры противодействия возникающим угрозам (в том числе и применить контрмеры к нападающим в процессе длящейся атаки), а также самостоятельно принять необходимые решения в процессе отражения длящейся атаки;
* загрузка дежурных специалистов, отвечающих за реагирование на инциденты, может быть крайне неравномерной.

### **1.13.1 Страхование информационных рисков. Основы методологии страхования информационных ресурсов**

Объектами страхования выступают:

* информационные ресурсы (в любом их виде: базы данных, библиотеки электронных документов и т.п.);программное обеспечение (как уже используемые программные собственные и покупные продукты, так и находящиеся в разработке);
* аппаратное обеспечение информационных систем (сетевое оборудование, серверы, рабочие станции, телекоммуникационное оборудование, периферия, источники бесперебойного питания и т.п.);
* финансовые активы (денежные средства, без документарные ценные бумаги) в электронной форме (в том числе средства на счетах, управляемых при помощи систем "клиент-банк").

Основные стадии процесса страхования информационных рисков представлены на рисунке 8:



**Рисунок 8 - Основные стадии процесса страхования информационных рисков**

## **1.14 Экономика информационной безопасности**

Особая сложность экономического анализа в такой сфере, как информационная безопасность, обуславливается такими специфическими факторами, как:

* быстрое развитие информационных технологий и методик, используемых в этой сфере (как средств и методов защиты, так и средств и методов нападения);
* невозможность достоверно предугадать все возможные сценарии нападения на информационные системы и модели поведения нападающих;
* невозможность дать достоверную, достаточно точную оценку стоимости информационных ресурсов, а также оценить последствия различных нарушений в денежном выражении.

В ситуации, когда необходимо осуществить некоторые новые организационные или технические мероприятия (реализовать проект), основной задачей лиц, отвечающих за эффективную организацию информационной безопасности, является четкое соотнесение затрат, которые придется понести в связи с реализацией этого мероприятия (как единовременные, так и постоянные текущие), и дополнительных (новых) денежных потоков, которые будут получены. В данном случае под денежным потоком может пониматься экономия затрат, предотвращение убытков, а также дополнительный доход предприятия.

В качестве основного показателя, отражающего это соотношение, в экономической практике принято использовать функцию отдачи от инвестиций – Return on Investment (ROI), указанная под формулой 1.

|  |  |
| --- | --- |
|  | (1) |

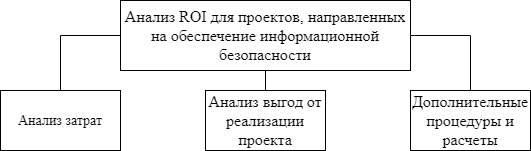
Где R - дополнительный денежный поток, создаваемый в результате реализации проекта, C - затраты, связанные с реализацией проекта (расход ресурсов, отрицательная величина), d - ставка дисконтирования, NVP - функция дисконтирования. А функция NVP(C, d) рассчитывается формулой 2:

|  |  |
| --- | --- |
|  | (2) |

Где T - предполагаемый жизненный цикл проекта (информационной и/или организационной системы), N - количество видов затрат, принимаемых в расчет, - затраты n-ого вида, понесенные в t-ом периоде, руб.

Функция дисконтирования используется при анализе инвестиционных вложений для учета влияния фактора времени и приведения разновременных затрат к одному моменту (моменту реализации проекта).

Модель отдачи от инвестиций акцентирует внимание на двух основных задачах, которые необходимо решить при анализе любого инвестиционного проекта и, в частности, проекта по реализации мероприятий в сфере информационной безопасности: расчет затрат, связанных с проектом, и расчет дополнительного денежного потока.



**Рисунок 9 - Структура методологии анализа эффективности вложений в проекты по обеспечению информационной безопасности**

Для осуществления такого анализа, как правило, используются следующие базовые понятия. Оценочная величина единовременных потерь (Single Loss Expectancy, ) – предполагаемая средняя оценочная сумма ущерба в результате одного нарушения информационной безопасности i-го типа. Она может быть определена как произведение общей стоимости защищаемых информационного активов (AV) на коэффициент их разрушения вследствие нарушения информационной безопасности(подверженности нападению), который обозначается (Exposure Factor).

Количество нарушений информационной безопасности за год(Annualized Rate of Occurrence, ) – оценочная частота, с которой втечение года происходят нарушения информационной безопасности(реализуются угрозы) i-го типа.

Оценочная величина среднегодовых потерь (Annualized Loss Expectancy, ) – суммарный размер потерь от нарушений информационной безопасности (реализации рисков) i-го типа в течение года.

|  |  |
| --- | --- |
|  | (3) |

Исходя из этого, общий денежный поток от реализации мероприятия определяется по следующей формуле:

|  |  |
| --- | --- |
|  | (4) |

Где R вычисляется формулой 5:

|  |  |
| --- | --- |
|  | (5) |

Несмотря на все трудности процесса оценки целесообразности внедрения средств защиты, описанная методология позволяет менеджерам и специалистам по защите информации получать обоснованные оценки и делать формализованные выводы относительно того, насколько оправданными являются вложения в определенные средства защиты информации, а также определить основные приоритеты расходования средств, предусмотренных в бюджете на обеспечение информационной безопасности.

Вывод В данной главе был проанализирован теоретический материал по ???.

ПОВТОРЮ, ОЧЕНЬ МНОГО ПОДПУНКТОВ

**СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ**

1. ГОСТ 7.32-2017. Межгосударственный стандарт. Система стандартов по информации, библиотечному и издательскому делу. Отчет о научно-исследовательской работе. Структура и правила оформления (введен в действие Приказом Росстандарта от 24.10.2017 N 1494-ст) – URL: http://docs.cntd.ru/document/1200157208 (дата обращения: 25.10.2020). – Текст: электронный.

2. ГОСТ 19.201-78. Межгосударственный стандарт. Единая система программной документации. Техническое задание. Требования к содержанию и оформлению (введен в действие Постановлением Госстандарта СССР от 18.12.1978 N 3351) (ред. от 01.06.1981) – URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=OTN&n=1815 (дата обращения: 24.10.2020). – Текст: электронный.

3. Анисимов, А. А. Менеджмент в сфере информационной безопасности : учебное пособие / А. А. Анисимов. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 211 c. — URL: http://www.iprbookshop.ru/89443.html (дата обращения: 25.10.2020). — Текст : электронный.