# Описание предприятия

Управление по делам гражданской обороны и чрезвычайным ситуациям.

Пользователей – 182.

Компьютеров –180.

Режим многопользовательский.

Есть выход в интернет под своим прокси-сервером.

Система распределенная.

Обрабатываемых данных больше 500 и меньше 5000.

Нужно защитить персональные данные.

Уровни конфиденциальности:

1. персональные данные;
2. пропуска;
3. информация для служебного пользования.

В организации имеются следующие должности:

1. Программисты;
2. Бухгалтеры;
3. Охраники;
4. Менеджеры;
5. Директор;
6. Директор охраны.

# Характеристика информационной системы предприятия

Все компьютеры имеют типовую конфигурацию:

- процессор -Intel(R) Celeron(R) CPU 2.80 GHz;  
- встроенный кэш L2 - 256Kb;  
- материнская плата - ASUS m3a;  
- ОЗУ - DIMM DDR 256Kb;  
- дисковод гибких дисков - LG;  
- жёсткий диск - SAMSUNG SV0411N(40068 MB);  
- CD-ROM/DVD - \_NEC CD-RW NR-9300A;  
- видеокарта - ATI Radeon9600;  
- принтер - BROTHER DCP-7065 DNR ;  
- операционная система - Microsoft Windows 7.

Компьютеры подключены к общей закрытой локальной сети делящейся на несколько уровней. На компьютерах расположенных в офисе установлено типовое программное обеспечение: Операционная система - Microsoft Windows 7 Профессиональная 5.01.2600 (Service Pack 3), пакет MS Office 2011, Эталон, Outlook.

Для автоматизации работы всех филлиалов РЖД, функционирующей на единой базе данных в закрытой вычислительной сети, используется программное обеспечение «Эталон».

**Задачи**

В данном индивидуальном задании практиканта поставлены следующие задачи:

1. определить цели и задачи защиты информации в организации;
2. составить матрицу доступа;
3. определить группу требований к автоматизированной системе (далее будет использовано сокращение АС);
4. определить предмет защиты на предприятии;
5. выявить возможные угрозы защищаемой информации в органе и их структуру;
6. выявить источники, виды и способы дестабилизирующего воздействия на защищаемую информацию на предприятии;
7. выявить каналы и методы несанкционированного доступа к защищаемой информации на предприятии;
8. определить основные направления, методы и средства защиты информации на предприятии.

# 1. Цели и задачи защиты информации

Целями защиты информации предприятия являются:

* предотвращение угроз безопасности;
* предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию конфиденциальной информации;
* предотвращение других форм незаконного вмешательства в информационные ресурсы и системы, обеспечение правового режима документированной информации как объекта собственности;
* сохранение, конфиденциальности документированной информации в соответствии с законодательством.

К задачам защиты информации на предприятии относятся:

* гарантия безопасности информации, ее средств, предотвращение утечки защищаемой информации и предупреждение любого несанкционированного доступа к носителям засекреченной информации;
* отработка механизмов оперативного реагирования на угрозы, использование юридических, экономических, организационных, социально-психологических, инженерно-технических средств и методов выявления и нейтрализации источников угроз безопасности предприятия;
* документирование процесса защиты информации, особенно сведений с тем, чтобы в случае возникновения необходимости обращения в правоохранительные органы, иметь соответствующие доказательства, что предприятие принимало необходимые меры к защите этих сведений.

# ****2. Требования по защите информации от НСД****

Защита информации от НСД является составной частью общей проблемы обеспечения безопасности информации. Мероприятия по защите информации от НСД должны осуществляться взаимосвязано с мероприятиями по специальной защите основных и вспомогательных средств вычислительной техники, средств и систем связи от технических средств разведки и промышленного шпионажа.

В общем случае, комплекс программно-технических средств и организационных (процедурных) решений по защите информации от НСД реализуется в рамках системы защиты информации от НСД, условно состоящей из следующих четырех подсистем:

* управления доступом;
* регистрации и учета;
* криптографической;
* обеспечения целостности.

Формализованные требования к защите компьютерной информации АС.

Существует 3 группы АС с включающими в себя требованиями по защите систем. Но, учитывая структуру органа, рассматривается первая группа АС (в соответствии с используемой в классификацией), как включающую в себя наиболее распространенные многопользовательские АС, в которых одновременно обрабатывается и/или хранится информация разных уровней конфиденциальности.

# 3. Объекты и предметы защиты

Основными объектами защиты в органе являются:

1. персонал (так как эти лица допущены к работе с охраняемой законом информацией либо имеют доступ в помещения, где эта информация обрабатывается);
2. объекты информатизации – средства и системы информатизации, технические средства приема, передачи и обработки информации, помещения, в которых они установлены, а также помещения, предназначенные для проведения служебных совещаний;
3. информация ограниченного доступа, а именно:

* отчетность служб экстренного реагирования.

1. защищаемая от утраты общедоступная информация:

* документированная информация, регламентирующая статус органа, права, обязанности и ответственность его работников (устав, журнал регистрации, положение о деятельности, положения о структурных подразделениях, должностные инструкции работников);

1. материальные носители охраняемой законом информации;
2. средства защиты информации (антивирусные программы, архиватор данных, программа для создания и восстановления резервной копии Windows, шифрование);

Предметом защиты информации в органе являются носители информации, на которых зафиксированы, отображены защищаемые сведения:

* база данных чрезвычайных происшествий;
* приказы, постановления, положения, инструкции, соглашения и обязательства о неразглашении, распоряжения, договоры, планы, отчеты, ведомость ознакомления с Положением о конфиденциальной информации и другие документы в бумажном и электронном виде.

# 4. Угрозы защищаемой информации

Внешние угрозы:

* несанкционированный доступ к информации (хакеры, взломщики)
* вирусы;
* чрезвычайные ситуации;
* шпионские программы (флешки и т.п.);
* несанкционированное копирование;
* кража программно-аппаратных средств.

Внутренние угрозы:

* разглашение конфиденциальной информации сотрудниками органа;
* нарушение целостности данных со стороны сотрудников органа;
* потеря информации на жестких носителях;
* угрозы целостности баз данных;
* угрозы целостности программных механизмов работы предприятия;
* делегирование лишних или неиспользуемых полномочий на носитель с конфиденциальной информацией, открытие портов;
* системные сбои;
* повреждение аппаратуры, отказ программного или аппаратного обеспечения;
* угрозы технического характера;
* угрозы нетехнического или некомпьютерного характера – отсутствие паролей, конфиденциальная информация, связанная с информационными системами хранится на бумажных носителях.

# 5. Источники, виды и способы дестабилизирующего воздействия на защищаемую информацию

К источникам дестабилизирующего воздействия относятся:

* люди;
* технические средства отображения (фиксации), хранения, обработки, воспроизведения, передачи информации, средства связи и системы обеспечения их функционирования;
* природные явления.

Виды и способы дестабилизирующего воздействия на защищаемую информацию дифференцируются по источникам воздействия. Самое большее количество видов и способов дестабилизирующего воздействия имеет отношение к людям**.**

Со стороны людей возможны следующие виды воздействия, приводящие к уничтожению, искажению и блокированию:

* непосредственное воздействие на носители защищаемой информации;
* несанкционированное распространение конфиденциальной информации;
* вывод из строя технических средств отображения, хранения, обработки, воспроизведения, передачи информации и средств связи;
* нарушение режима работы перечисленных средств и технологии обработки информации;
* вывод из строя и нарушение режима работы систем обеспечения функционирования названных средств.

Несанкционированное распространение конфиденциальной информации может осуществляться путем*:*

* словесной передачи (сообщения) информации;
* передачи копий (снимков) носителей информации;
* показа носителей информации;
* ввода информации в вычислительные сети;
* опубликования информации в открытой печати;
* использования информации в открытых публичных выступлениях, в т.ч. по радио, телевидению;
* потеря носителей информации.

Способами нарушения режима работы технических средств отображения, хранения, обработки, воспроизведения, передача информации, средств связи и технологии обработки информации, приводящими к уничтожению, искажению и блокированию информации, могут быть:

* повреждение отдельных элементов средств;
* нарушение правил эксплуатации средств;
* внесение изменений в порядок обработки информации;
* заражение программ обработки информации вредоносными программами;
* выдача неправильных программных команд;
* превышение расчетного числа запросов;
* передача ложных сигналов – подключение подавляющих фильтров в информационные цепи, цепи питания и заземления;
* нарушение (изменение) режима работы систем обеспечения функционирования средств.

К видам дестабилизирующего воздействия на защищаемую информацию со стороны технических средств отображения, хранения, обработки, воспроизведения, передачи информации и средств связи и систем обеспечения их функционирования относятся:

* выход средств из строя;
* сбои в работе средств
* создание электромагнитных излучений.

# 6. Каналы и методы несанкционированного доступа к защищаемой информации

информация защита несанкционированный

К числу наиболее вероятных каналов утечки информации можно отнести:

* визуальное наблюдение;
* подслушивание;
* техническое наблюдение;
* прямой опрос, выведывание;
* ознакомление с материалами, документами;
* сбор открытых документов и других источников информации;
* хищение документов и других источников информации;
* изучение множества источников информации, содержащих по частям необходимые сведения.

# 

# 7. Организация комплексной системы защиты информации

Для организации эффективной защиты конфиденциальной информации необходимо разработать программу, которая должна позволить достигать следующие цели:

* обеспечить обращение сведений в заданной сфере;
* предотвратить кражу и утечку конфиденциальной информации, любую порчу конфиденциальной информации;
* документировать процесс защиты данных, чтобы в случае попыток незаконного завладения какими-либо данными предприятия можно было защитить свои права юридически и наказать нарушителя.

Система доступа к конфиденциальным данным, должна обеспечить безусловное ознакомление с такими материалами только тех лиц, которым они нужны по службе. Система доступа к конфиденциальной информации – есть комплекс административно-правовых норм, обеспечивающих получение необходимой для работы информации каждым исполнителем и руководителем секретных работ. Цель системы – обеспечить только санкционированное получение необходимого объема конфиденциальной информации. В структуру этой системы входят:

* разрешительная система доступа к документальной конфиденциальной информации;
* система пропусков и шифров, обеспечивающая только санкционированный доступ в помещения, где ведутся секретные работы.

Для обеспечения физической сохранности носителей засекреченной информации и предотвращения доступа посторонних лиц нужна система охраны, которая включает в себя комплекс мероприятий, сил и средств, задействованных для преграждения доступа посторонних лиц к носителям защищаемой информации.

# 

# Заключение

В процессе выполнения индивидуального задания практикантам была поставлена задача – создать и проанализировать средства информационной безопасности предприятия. Поставленные цели были достигнуты при помощи классифицирования предприятия, были предложены методы и средства для усовершенствования политики безопасности данного предприятия, в результате выполнения которых предприятие позволит повысить эффективность средств защиты и сократит риск потери и искажения информации.

Следует обратить внимание на то, что только при совместном взаимодействии персонала, программно-аппаратных средств и средств защиты информации возможна эффективность данных мероприятий.

Данное предприятие циркулирует большим количеством информации конфиденциального характера, доступ к которой необходимо ограничить. Поэтому, целью являлась разработка такой системы по защите информации, при которой угрозы утечки конфиденциальной информации были бы минимальны.

В результате анализа была построена модель информационной системы с позиции безопасности.

Никакие аппаратные, программные и любые другие решения не смогут гарантировать абсолютную надежность и безопасность данных в компьютерных сетях. В то же время свести риск потерь к минимуму возможно лишь при комплексном подходе к вопросам безопасности.