1. Описание организации

Организация “АО Алмаз”
Пользователей – 240.
Компьютеров – 270.
Режим многопользовательский.
Есть выход в интернет.
Система распределенная.
Обрабатываемых данных больше 5000 и меньше 80000.
Нужно защитить персональные данные.
Организация включает в себя следующие отделы:

1. Администрация;
2. Бухгалтерия;
3. Отдел информационных технологий;
4. Отдел финансирования;
5. Отдел закупок;
6. Производственно-технический отдел;
7. Отдел кадров;
8. Отдел стратегического развития;
9. Производственный цех;

Уровни конфиденциальности;

1. Персональные данные;
2. Информация для служебного пользования;
3. Засекреченная информация;

В организации имеются следующие должности;

1. генеральный директор;
2. заместитель генерального директора;
3. главный бухгалтер;
4. секретарь;
5. Начальник отдела стратегического развития;
6. Специалист по маркетингу;
7. Экономист в отдел внешней комплектации;
8. Инженер по подготовке производства;
9. Монтажник
10. Шлифовщик
11. Токарь

Характеристика информационной системы организации

Организация использует следующее программное обеспечение:

– пакет Microsoft Office;
– 1С Предприятие 8.3 конфигурация бухгалтерия предприятия.
– 1С ЗУП 3.0 (зарплата и управление персоналом);
– VMware vSphere

Все рабочие места сотрудников оснащены компьютерами с разграниченными правами доступа:

- генеральный директор анализирует работу организации, планирования деятельности и т.п.,
- заместитель генерального директора наделен теми же полномочиями, что и генеральный директор;
- главный бухгалтер рассчитывает заработную плату, ведет учет ведения оказанных услуг, основных средств, товарно-материальных ценностей, расчеты с поставщиками и заказчиками, учет денежных средств организации, расчет налогов;
- секретарь имеет доступ к договорам, входящей и исходящей корреспонденции.
- начальник ОИТ контролирует работу сотрудников ОИТ, планирует график технического обслуживания компьютеров на предприятии, осуществляет контроль за своевременной аттестацией подчиненных;
- Инженер по подготовке производства контролирует работу сотрудников цеха, осуществляет контроль за сроками своевременной аттестации подчиненных;
- отделы: финансирования, кадров, закупок стратегического развития предприятия имеют доступ к текстовым и графическим редакторам;

Все компьютеры подключены к локальной сети организации, вход в систему осуществляется с помощью персональных логинов и паролей пользователей.

Для безопасного доступа пользователей локальной сети в Интернет, для защиты компьютеров от вторжений хакеров, вирусов, спама, точного подсчета трафика используется Интернет-шлюз «Интернет Контроль Сервер» на платформе Windows. В состав программного обеспечения входят прокси-сервер, межсетевой экран, антивирусная защита, система обнаружения атак, система анализа содержимого трафика, анти-спам.

Для защиты помещений от несанкционированного доступа, на территории организации установлены камеры видеонаблюдения, система сигнализации, система противопожарной безопасности.

Актуальность проблемы защиты информации в организации

Обеспечение защиты информации в организации предусматривает необходимость защиты персональных данных. Наиболее важной представляется защита персональных данных, так как доверие заказчиков в первую очередь основывается на предоставлении своих личных данных, и соответственно, сохранением их сотрудниками организации.

Поэтому целью обеспечения безопасности в организации является разработка политики безопасности и обеспечение надежной защиты информации для его нормального функционирования.

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 в организации;
5. выявить возможные угрозы защищаемой информации в организации и их структуру;

6. выявить источники, виды и способы дестабилизирующего воздействия на защищаемую информацию в организации;

7. выявить каналы и методы несанкционированного доступа к защищаемой информации в организации;

8. определить основные направления, методы и средства защиты информации в организации.

2. Цели и задачи защиты информации в организации

Целями защиты информации организации являются:

– предупреждение хищения, утечки, утраты, искажения, подделки конфиденциальной информации (персональных данных);

– предотвращение угроз безопасности личности и организации;

– 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;

– защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;

– сохранение, конфиденциальности документированной информации в соответствии с законодательством.

К задачам защиты информации на предприятии относятся:

– обеспечение управленческой, финансовой и маркетинговой деятельности организации режимным информационным обслуживанием, то есть снабжением всех служб, подразделений и должностных лиц необходимой информацией, как засекреченной, так и несекретной. При этом деятельность по защите информации по возможности не должна создавать больших помех и неудобств в решении производственных и прочих задач, и в то же время способствовать их эффективному решению, давать предприятию преимущества перед конкурентами и оправдывать затраты средств на защиту информации.

– 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 организации;

– документирование процесса защиты информации, особенно сведений с тем, чтобы в случае возникновения необходимости обращения в правоохранительные органы, иметь соответствующие доказательства, что организация принимала необходимые меры к защите этих сведений;

– организация специального делопроизводства, исключающего несанкционированное получение конфиденциальной информации.

3. Матрица доступа

Основой политики безопасности является избирательное управление доступом, которое подразумевает, что все субъекты и объекты системы должны быть идентифицированы; права доступа субъекта к объекту системы определяются на основании некоторого правила (свойство избирательности).

Для описания свойств избирательного управления доступом применяется модель системы на основе матрицы доступа (МД), иногда ее называют матрицей контроля доступа. Матрица доступа представляет собой прямоугольную матрицу, в которой объекту системы соответствует строка, а субъекту столбец. На пересечении столбца и строки матрицы указывается тип разрешенного

доступа субъекта к объекту. Обычно выделяют такие типы доступа субъекта к объекту, как «доступ на чтение», «доступ на запись», «доступ на исполнение» и др.

Множество объектов и типов доступа к ним субъекта может изменяться в соответствии с некоторыми правилами, существующими в данной системе. Определение и изменение этих правил также является задачей МД.

Начальное состояние системы определяется матрицей доступа, все действия регламентированы и зафиксированы в данной матрице.

R – чтение из объекта;

W – запись в объект;

CR – создание объекта;

D – удаление объекта;

“+” – определяет права доступа для данного субъекта;

“–” – не определяет права доступа для данного субъекта.

Состояние системы считается безопасным, если в соответствии с политикой безопасности субъектам разрешены только определённые типы доступа к объектам (в том числе отсутствие доступа).

Объектами защиты на предприятии являются:

O1 – технические средства приема, передачи и обработки информации;

O2 – персональные данные заказчиков;

O3 – персональные данные работников;

O4 – документированная информация;

O5 – личные дела работников;

O6 – электронные базы данных работников и заказчиков;

O7 – средства защиты информации (антивирусные программы, система сигнализации, система противопожарной охраны и др.);

Субъектами доступа к ресурсам организации являются:

S1 – генеральный директор;

S2 – заместитель генерального директора;

S3 – главный бухгалтер;

S4 - секретарь;

S5 – Начальник отдела стратегического развития;

S6 – Специалист по маркетингу;

S7 – Экономист ;

S8 – Инженер по подготовке производства;

Таблица 1. Матрица доступа

	O1	O2	O3	O4	O5	O6	O7	S1	S2	S3	S4	S5	S6	S7	S8
S1	R,W,CR,D	R,W,CR,D	R,W,CR,D	R,W,CR,D	R,W,CR,D	R,W,CR,D	R,W,CR,D	+	-	-	-	-	-	-	-
S2	R,W,CR,D	R,W,CR,D	R,W,CR,D	R,W,CR,D	R,W,CR,D	R,W,CR,D	R,W,CR,D	-	+	-	-	-	-	-	-
S3	R,W,CR,D	R,W,CR,D	R,W,CR,D	R,W,CR,D	R,W,CR,D	R,W,CR,D	R,W,CR,D	-	-	+	-	-	-	-	-
S4	R	R	R,W	RW	-	R	R,W,	-	-	-	+	-	-	-	-
S5	R,W	R,W	-	R,W	-	-	R	-	-	-	-	+	-	-	-
S6	R	-	-	R,W	-	-	R	-	-	-	-	-	+	-	-
S7	R,W,CR	R,W	-	R,W,CR	-	-	R	-	-	-	-	-	-	+	-
S8	R,W	R,W	-	R,W	-	-	R	-	-	-	-	-	-	-	+

4. 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 организации, рассматривается первая группа АС (в соответствии с используемой классификацией), как включающую в себя наиболее распространенные многопользовательские АС, в которых одновременно обрабатывается и/или хранится информация разных уровней конфиденциальности. Причем не все пользователи имеют право доступа ко всей информации АС.

5. Объекты и предметы защиты в организации

Основными объектами защиты в организации:

1. персонал (так как эти лица допущены к работе с охраняемой законом информацией (персональные данные) 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:

- персональные данные работников (фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное положение, образование, профессия, уровень квалификации, доход, наличие судимостей и некоторая другая информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника);
- персональные данные заказчиков (наименование заказчика, персональные данные должностных лиц, сведения о расчетных счетах заказчиков);

4. защищаемая от утраты общедоступная информация:

- документированная информация, регламентирующая статус организации, права, обязанности и ответственность его работников (устав, журнал регистрации, учредительный договор, положение о деятельности, положения о структурных подразделениях, должностные инструкции работников);
- информация, которая может служить доказательным источником в случае возникновения конфликтных ситуаций (расписки);

5. материальные носители охраняемой законом информации (личные дела работников, сведения о заказчиках, электронные базы данных работников и заказчиков, бумажные носители и электронные варианты приказов, постановлений, планов, договоров, отчетов);
6. средства защиты информации (антивирусные программы, архиватор данных, программа для создания и восстановления резервной копии Windows, шифрование);
7. технологические отходы (мусор), образовавшиеся в результате обработки охраняемой законом информации (данные о бывших заказчиках и сотрудниках).

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

- база данных о заказчиках и сотрудниках организации в бумажном и электронном виде;

– 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.

6. Угрозы защищаемой информации в организации

Внешние угрозы:

– конкуренты;
– 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 организации;
– нарушение целостности данных со стороны персонала организации;
– потеря информации на жестких носителях;
– угрозы целостности баз данных;
– угрозы целостности программных механизмов работы организации;
– 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.

7. 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.

8. Каналы и методы несанкционированного доступа к защищаемой информации в организации

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.

9. Организация комплексной системы защиты информации в организации

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 организации можно было защитить свои права юридически и наказать нарушителя.

Программа будет отражать размер данной организации, тип технологии и деловой информации, которую необходимо защищать.

В программе должны учитываться возможные источники и каналы утечки информации.

Для построения системы защиты конфиденциальной информации на предприятии необходимо создание службы защиты информации (далее – СлЗИ), которая будет являться

структурной единицей организации, непосредственно участвующей в производственно-коммерческой деятельности. Работа этого отдела проводится во взаимодействии со структурными подразделениями организации. Структура и штат СлЗИ в зависимости от объема работ и особенностей производственно-коммерческой деятельности определяются руководителем организации и, как правило, должны комплектоваться инженерно-техническими работниками – специалистами основного профиля работы данной организации, а также специалистами, имеющими практический опыт защиты информации или работы с различными группами людей. Назначение на должность начальника СлЗИ организации, а также его освобождение производится только руководителем организации. Руководитель службы защиты информации регулярно, в установленные сроки отчитывается в своей работе перед директором организации.

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 организации ООО «АО Алмаз». Поставленные цели были достигнуты при помощи классифицирования организации, были предложены методы и средства для усовершенствования политики безопасности данной организации, 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.