Содержание:

1. Введение в проблему
2. Резюме продукта
3. Угрозы и уязвимости на предприятии
4. Фактическая защищенность предприятия
5. Возможные каналы утечки информации
6. Предлагаемые мероприятия по защите
7. Объекты поставки проекта
8. Оценка стоимости системы защиты и оценка эффективности
9. Предложение, ограничения, исключения
10. Структура разбиения работ
11. Структурная схема организации
12. Матрица ответственности
13. Сетевой график и диаграмма Ганта
14. Риски проекта

15.Заключение

1. **Введение в проблему**

Эффективное управление проектами — это интеграция информационных систем планирования с управленческими процедурами и организационной структурой. При этом покупка удачного программного обеспечения не равносильна успешной постановке управления проектами в организации.

Для эффективного управления проектом создания системы информационной безопасности необходимо преобразовать проект в последовательность действий имеющих четко определенные цели, ограниченных во времени и допускающих независимые процедуры верификации. В принципе мониторинг процесса может осуществлять один человек, но высокая критичность принятых решений и их глубокая взаимосвязь с важнейшими бизнес-процессами компании требует принятия взвешенных решений с участием максимально возможного (с точки зрения обеспечения оперативности) числа задействованных лиц.

Среди основных признаков проекта можно выделить:

* уникальность и неповторимость целей и работ проекта;
* координированное выполнение взаимосвязанных работ;
* направленность на достижение конечных целей;
* ограниченность во времени (наличие начала и окончания);
* ограниченность по ресурсам.

Любой проект существует не изолированно, а в окружении множества различных субъектов и, соответственно, под влиянием оказываемого ими влияния.

Проект имеет ряд свойств: возникает, существует и развивается в определенном окружении, называемом внешней средой, состав проекта не остается неизменным в процессе его реализации и развития: в нем могут появляться новые элементы (объекты) и удаляться из его состава другие элементы.

Без Комплексной системы защиты информации ни одно предприятие не сможет вести успешную деятельность.

В рассмотренной мною фирма «ИТ Энигма» циркулирует большое количество информации конфиденциального характера доступ к которой необходимо ограничить. Поэтому, необходимо разработать такую систему по защите информации, при которой угрозы утечки конфиденциальной информации будут минимальны. При этом на предприятии уже имеются некоторые меры по защите информации.

1. **Резюме продукта**

Компания «ИТ Энигма» представляет широкий спектр услуг:

- диагностика защищенности компьютерных систем

- аудит безопасности корпоративных сетей

- сопровождение и поддержка безопасности информационных систем

- аттестация объектов информатизации на соответствие требованиям по обработке конфиденциальной информации

- и тд.

На предприятии циркулируют сведения конфиденциального характере, такие как: коммерческая тайна, персональные данные, информация для служебного пользования.

Клиентами компании является большое количество крупных организаций, среди которых:

- Цинковый завод (г.Челябинск)

[- Областной радиотелевизионный передающий центр (г.Челябинск)](http://www.it-enigma.ru/clients.html)

[- Промышленная группа "Ричел" (г.Челябинск)](http://www.uk.richel.ru)

[- Компания "Фрост-Инвест" (г.Челябинск)](http://www.it-enigma.ru/clients.html)

[- ООО "Финансовое агентство "Милком-Инвест" (г.Челябинск)](http://www.milcom.ru)

[- ОАО "Уралинвестэнерго" (г. Екатеринбург.)](http://www.it-enigma.ru/clients.html)

[- Южноуральская регистрационная палата (г. Челябинск)](http://www.it-enigma.ru/clients.html)

[- ООО "Аеросервис (г. Челябинск)](http://www.aeroservice.su/)

Основными документами конфиденциально характера на предприятии являются:

1. Приказ о мерах защиты
2. Приказ о назначении комиссии по подготовке и обеспечению проведения аттестации объектов информатизации
3. Приказ о категорировании и классификации объектов вычислительной техники
4. Приказ о вводе в эксплуатацию ПЭВМ
5. Приказ о введении режима коммерческой тайны на предприятии
6. Положение о службе безопасности фирмы
7. Положение об отделе администрирования и технического сопровождения информационных систем
8. Положение об определении требований по защите (категорированию) ресурсов автоматизированной системы организации
9. Положение о группе инженерно-технической защиты информации
10. Положение об охранно-пропускном режиме предприятия
11. Положение о структуре службы безопасности
12. Положение об отделе защиты информации
13. Положение о компьютерной сети организации
14. Положение о системном администрировании компьютерной сети организации
15. Концепция обеспечения безопасности информации в автоматизированной системе организации
16. Нормативно-методическая документация по осуществлению деятельности, связанной с проведением аттестации объектов
17. Должностные инструкции сотрудников предприятия
18. Трудовые договоры сотрудников, работающих с конфиденциальной информацией
19. Список постоянных пользователей определенного ПЭВМ, допущенных в помещение, и установленные им права доступа к информации и техническим ресурсам ПЭВМ
20. Перечень сотрудников предприятия, имеющих доступ у средствам АС и к обрабатываемой на них информации
21. Генеральный план развития организации
22. План инвестиций предприятия
23. Бюджет организации
24. Долговые обязательства предприятия
25. Отчет об уровне доходов предприятия
26. Отчет об уровне выручки предприятия
27. Договор подряда на режимное обслуживание клиентов
28. Договоры предоставления услуг
29. Договоры, заключенные с поставщиками оборудования
30. Договоры, заключенные с клиентами

Внутренними субъектами доступа к информационным ресурсам предприятия являются:

А) Сотрудники организации, пользователи внутренней корпоративной сети, наделенные полномочиями и уровнем доступа, необходимым для осуществления непосредственной деятельности

Б) Администраторы внутренней сети и служба безопасности организации, осуществляющие контроль над безопасностью внутренней сети организации

Основными объектами защиты на предприятии « ИТ Энигма» являются: конфиденциальная информация, автоматизированные рабочие места

Конфиденциальная информация в структурных подразделениях предприятия обрабатывается с помощью офисных приложений, специального программного обеспечения с использованием систем управления базами данных.

На предприятии «ИТ Энигма» уже существуют некоторые меры по защите информации:

1. Автоматизированные рабочие места, на которых производится работа с конфиденциальной информацией, не подсоединены к сети Internet
2. Существует режим и инструкция по противопожарной безопасности
3. На главном входе установлена камера видеонаблюдения
4. Существует график посещений
5. На АРМ установлено противовирусное программное обеспечение
6. Существует перечень конфиденциальной информации
7. Существуют должностные инструкции сотрудников
8. Каждое АРМ имеет свой личный пароль входа
9. На окнах установлены решетки
10. Каждое рабочее место отделено перегородкой, затрудняющей просмотр находящейся на мониторе и на рабочем столе информации
11. На дверях в кабинет директора установлены автоматические доводчики.

На сервере и рабочих местах применяются операционные системы MS Windows, что позволяет применить сертифицированные средства защиты от НСД.

Возможна утечка информации по каналам ПЭМИН, по эфиру, по кабелям, выходящим за пределы КЗ.

1. **Угрозы и уязвимости на предприятии**
2. Автоматизированное рабочее место сотрудника

|  |  |
| --- | --- |
| Угроза | Уязвимости |
| 1.Физический доступ нарушителя к рабочему месту | 1. Отсутствие системы контроля доступа сотрудников к чужим рабочим местам |
| 2.Отсутствие системы видеонаблюденияВ организации |
| 3. Несогласованность в системе охраны периметра |
| 2.Разглашение конфиденциальной информации, хранящейся на рабочем месте сотрудника организации | 1.Отсутствие соглашения о неразглашении между работником и работодателем  |
| 2.Нечеткое регламентация ответственности сотрудников предприятия |
| 3.Разрушение (повреждение, утрата) конфиденциальной информации при помощи специализированных программ и вирусов | 1.Отсутствие антивирусного программного обеспечения  |
| 2.Отсутствие ограничения доступа пользователей к сети интернет, внутренней сети предприятия |

1. Серверная комната

|  |  |
| --- | --- |
| Угроза | Уязвимости |
| 1.Физический неавторизованный доступ нарушителя в серверную комнату | 1.Неорганизованный контрольно-пропускной режим в организации |
| 2.Отсутствие видеонаблюдения в серверной комнате |
| 2.Разглашение конфиденциальной информации, хранящейся на сервере | 1.Отсутствие соглашения о нераспространении конфиденциальной информации |
| 2. Нечеткая регламентация ответственности сотрудников предприятия |

1. Конфиденциальная информация

|  |  |
| --- | --- |
| Угроза | Уязвимости |
| 1.Физический доступ нарушителя к носителям | 1.Неорганизованность контрольно-пропускного режима в организации |
| 2.Отсутствие видеонаблюдения в организации |
| 2.Разглашение конфиденциальной информации, используемой в документах, вынос носителей за пределы контролируемой зоны | 1.Отсутствие соглашения о неразглашении конфиденциальной информации  |
| 2. Нечеткое распределение ответственности за документы (носители конфиденциальной информации) между сотрудниками организации |
| 3.Несанкционированное копирование, печать и размножение носителей конфиденциальной информации | 1. Нечеткая организация конфиденциального документооборота в организации  |
| 2. Неконтролируемый доступ сотрудников к копировальной и множительной технике |

## Фактическая защищенность организации

На предприятии ООО «ИТ Энигма» на данный момент реализованы следующие мероприятия:

Организационные мероприятия:

1. Доступ в кабинет руководителя в его отсутствие осуществляется только в присутствии секретаря. Ключ от помещений хранится у секретаря.
2. Во все помещения фирмы имеют доступ лишь персонал организации и клиенты, заключившие договор на оказание услуг с предприятием.
3. Посетители, ожидающие приема, находятся в приемной под присмотром секретаря. Ожидающим запрещено проходить дальше приемной без разрешения руководителя организации.
4. Вход людей в здание осуществляется через контрольно-про­пускной пункт на 1-ом этаже здания. Охрана на КПП организована ЧОП «ХХХ», парковка автотранспорта неограниченна.
5. Вход людей в помещение предприятия ООО «ИТ Энигма» осуществляется через двустворчатую металлическую дверь с видеодомофоном и магнитным ключом. Для входа в помещение сотрудники организации используют ключи, посетители пользуются видеодомофоном.

Правовые мероприятия:

1. Существуют инструкции для сотрудников, допущенных к защищаемым сведениям,
2. Инструкции сотрудников , ответственных за защиту информации
3. Утверждены должностные обязанности руководителей, специалистов и служащих предприятия
4. Существует положение о порядке обращения с информацией
5. Существует положение об отделе защиты информации
6. Разработана памятка пользователя АС

Инженерно-технические меры:

1. Во всех помещениях организации установлены извещатели пожарной сигнализации
2. На входной двери в помещение организации установлена камера , позволяющая видеть посетителей у входа
3. Электропитание здания осуществляется от трансформаторной подстанции, которая расположена на неконтролируемой территории и обслуживается сторонней организацией
4. Система кондиционирования, состоящая из 3х кондиционеров не защищена
5. Отсутствуют датчики вибро-акустического зашумления на стояках отопления, выходящих за пределы КЗ
6. Генераторы электромагнитного шума в помещении не установлены
7. Окна организации выходят во двор. На окнах имеются жалюзи, но отсутствуют вибрационные датчики.
8. Мероприятия по обнаружению «закладок» на территории КЗ проводятся 1 раз в пол года
9. Отсутствует защита телефонных линий.

Программно-аппаратные меры:

1. На АРМ сотрудников установлены операционная система - MS Windows XP, офисное приложение – MS Office 2007, антивирусное программное обеспечение – NOD32, 1С «Бухгалтерия» (в отделе бухгалтерия).
2. На АРМ установлена программа регистрации входа/выхода, а также всех произведенных действий с учетом времени.

## 5. Возможные каналы утечки информации

1. Распространение акустических сигналов через двери

2. Распространение вибрационных сигналов через стены с соседними помещениями, через трубы системы отопления и через окна

3. Разглашение информации сотрудниками предприятия умышленно или а следствии недостаточного знания работниками организации правил защиты конфиденциальной информации

4. Перехват акустической (речевой ) информации при помощи разнообразных средств разведки: микрофоны, радиомикрофоны , радиозакладки

5. Оптический просмотр через окна

6. Необходимо увеличить защиту на АРТ сотрудников организации

**6. Предполагаемые мероприятия по защите информации**

1. Уплотнение всех дверей на территории КЗ, кроме входной.

2. Мероприятия по выявлению закладных устройств проводить 1 раз в месяц.

3. Установление вибрационных генераторов на трубы системы отопления.

4. Установить вибрационные генераторы на окна (с целью уменьшения риска снятия лазером информации с окон).

5. Установит генераторы электромагнитного шума на каждое АРМ.

6. Разработать инструкцию пользователя ОВТ (объекта вычислительной техники).

7. Усовершенствовать инструкцию по организации парольной защиты на АРМ

8. Провести инструктаж персонала в соответствии с новой КСЗИ.

9. Разработать «Соглашение о неразглашении конфиденциальной информации»; провести инструктаж по разъяснению персоналу организации положений «Памятки».

10. Разграничить доступ пользователей АС к информации с помощью установки СЗИ от НСД на рабочих местах и сервере (СЗИ SecretNet);

11. На время проведения совещаний отключать телефонные аппараты от сети;

12. При проведении совещаний и переговоров отключать мобильные телефоны всем присутствующим в помещении.

13. Ключи и коды от сейфов должны храниться у руководителя предприятия.

14. Обязательно выключение компьютеров после завершения рабочего дня.

1. **Объекты поставки проекта**

Для управления проектом его следует разбить на иерархические подсистемы и компоненты. В терминах управления проектами структура проекта представляет собой "дерево" ориентированных на продукт проекта компонентов, представленных оборудованием, работами, услугами и информацией, полученными в ходе реализации проекта. Можно сказать, что структура проекта – это организация связей и отношений между его элементами. Формирование структуры проекта позволяет представить его в виде значительно меньших блоков работ вплоть до получения самых мелких, поддающихся непосредственному контролю позиций. Именно такие блоки передаются под управление отдельным специалистам, ответственным за достижение конкретной цели достигаемой при реализации задач данного блока. Процесс структуризации является неотъемлемой частью общего процесса планирования проекта и определения его целей, а также подготовки плана проекта и матрицы распределения ответственностей и обязанностей.

Задачей проекта является построение надежной системы защиты информации на предприятии.

Для предприятия «ИТ Энигма» в ходе разработки комплексной системы защиты информации необходимо выделить несколько задач в пределах следующих требований:

1. Техническое оснащение объекта должно сводить к минимуму возможность снятия конфиденциальной информации по возможным каналам утечки
2. Техническое оснащение должно удовлетворять требованиям и нормам стандартов в области защиты информации
3. Техническое оснащение не должно мешать рабочему процессу предприятия
4. Должна быть проведена оценка защищенности АРМ в соответствии с требованиями стандартов
5. Должны быть разработаны должностные инструкции в соответствии с поставленными задачами и формами допуска к конфиденциальной информации
6. По завершении работ по построению комплексной системы защиты информации необходимо провести ознакомление сотрудников с новой системой.

Итогом работы по построение КСЗИ должно быть:

1. Защита контролируемой зоны от проникновения злоумышленников и несанкционированного съема информации
2. Создание собственной политики безопасности предприятия
3. Строгий контроль доступа к конфиденциальной информации на электронный и бумажных носителях, к АРМ содержащим конфиденциальную информацию
4. Технического оснащения помещений, в которых ведется работа с конфиденциальными документами
5. Введение строгого учета конфиденциальной документации
6. Введение системы ответственности за невыполнения норм и требований по работе с конфиденциальной информацией.

**8.Оценка стоимости системы защиты и оценка эффективности**

Примерная стоимость работ и оборудования СЗИ:

|  |  |
| --- | --- |
| Статья затрат | Стоимость, руб. |
| 1. Приобретение средств защиты  | 950 000 |
| 2. Монтаж СЗИ  | 55 000 |
| 3. Специсследования помещений | 40 500 |
| 4.Надбавки к заработным платам сотрудников | 150 000 |
| 5. Разработка заключения о степени защищенности и аттестата соответствия | 15 000 |
| **Итого:** | 1210500 |

Таким образом из приведенных выше расчетов видно, что в случае реализации угроз на каждый из 3-х ресурсов предприятие понесет убытки:

49300\*20+159200+48200\*3=1193400 руб.

При этом следует отметить, что срок эксплуатации средств защиты превышает 1 год и система ЗИ рассчитана на более длительный срок.

Следовательно построение КСЗИ на предприятии ООО «ИТ Энигма» можно считать экономически целесообразным.

**9.Предложение, ограничения, исключения**

При построении системы защиты необходимо учитывать все каналы утечки информации. Всегда следует помнить, что злоумышленник не обязательно может получить весь объем конфиденциальной информации, используя только какой-либо один канал утечки информации. Следовательно, нужно обеспечивать блокирование каналов утечки комплексно.

Наибольшую опасность представляет оптический канал утечки информации. Связано это с тем, что практически вся информация может быть представлена в визуальном виде, неважно, что это: бумажные документы или электронный документ, отображённый на экране монитора. Следовательно, любая эта информация может быть сфотографирована. А развитие современных средств фотографии привело к тому, что даже на очень большом расстоянии, например при спутниковой фотосъемке, изображение имеет высокое разрешение. К тому же фотография содержит наибольшее количество демаскирующих признаков, такие как габариты, цвет, общий внешний вид и т.д. Однако стоит отметить, что в первую очередь фотография предназначена для добывания видовых демаскирующих признаков.

Для добывания сигнальных демаскирующих признаков используется радиоэлектронный канал утечки информации. В то же время вследствие различных характеристик каналов утечки информации, а также передаваемой по ним информации для получения конфиденциальной, и для повышения эффективности добывания конфиденциальной все каналы утечки информации используются комплексно. При этом злоумышленник получает возможность не только добыть информацию в максимальном объеме, но и может путём сопоставления информации, полученной из различных каналов добывания, оценить её достоверность. При организации защиты информации следует помнить об этом и предусмотреть использование злоумышленником нескольких каналов утечки информации.

Каналы утечки информации можно квалифицировать на следующие группы:

-визуально-оптические;

-акустические (включая и акустико-преобразовательные);

-радиоэлектронные;

-материально-вещественные (бумага, фото, магнитные носители).

Блокирование оптического канала утечки информации возможно с помощью организационных средств:

* На время проведения конфиденциальных совещаний и переговоров жалюзи должны закрываться
* При приёме посетителей на столе не должно находиться конфиденциальных документов, если в этом нет необходимости
* Телевизор не должен быть развёрнут экраном к окну
* Во время проведения конфиденциальных совещаний дверь должна быть плотно закрыта, а в идеале около двери должен постоянно находиться доверенный сотрудник компании, например, секретарь

Источником акустического сигнала могут быть:

* Говорящий человек
* Технические средства звуковоспроизведения
* Механические узлы технических средств и машин

Речь человека характеризуется рядом параметров:

* Громкость звука. Представляет собой взвешенную по частоте интенсивность звука.
* Тоновый диапазон или диапазон частот. Обычно тоновый диапазон составляет от 64 до 1300 Гц. Самые низкие тоны басовых голосов составляют около 40 Гц, а высокие тоны детских голосов могут достигать 4000 Гц.
* Тембр голоса человека определяется количеством и величиной гармоник (обертонов) его спектра.

Для предотвращения утечки информации по акустическому каналу необходимо применение специальных мер:

* Установка оконных блоков с повышенной звукоизоляцией (тройной стеклопакет)
* Заполнение пространства между стеклами специальными инертными газами
* Уплотнение притворов переплётов
* Установка окон в раздельные рамы
* Уплотнение притворов, что позволит увеличить величину звукоизоляции примерно на 5-10 дБ
* Изготовление двери из специальных звукоизолирующих материалов, что позволит дополнительно увеличить звукоизоляцию на 5-15 дБ
* Организация тамбуров с облицовкой внутреннего пространства тамбура звукопоглощающими материалами
* Организация в тамбурах воздушных пушек для создания хаотических воздушных потоков.

В защищаемом помещении источниками акустоэлектронного т канала утечки информации являются:

* Электропровода
* Провода пожарной и охранной сигнализации
* Радиопровода
* Телефонные провода
* Провода системы звукоусиления

Для блокирования акустоэлектронного канала утечки следует использовать приборы зашумляющие цепи электропитания и слаботочные цепи, а также подавители диктофонов и сотовых телефонов:

* Соната-С1 и Импульс – линейное зашумление цепей электропитания
* Мозаика – для блокирования сотовых телефонов всех стандартов
* Дурман – подавление сигналов ленточных и цифровых диктофонов

МП-2, МП-3, МП-5 – для подавления опасных сигналов в громкоговорителях, цепях

Материально-вещественным каналом утечки информации выступает документация. Скрытие этого канала утечки информации в первую очередь регулируется на организационном уровне, выработкой определенных правил обращения с бумажными носителями.

1. **Структура разбиения работ**

|  |  |  |
| --- | --- | --- |
| Наименование работы | Продолжи-тельность, maxДни | Продолжи-тельность, minдни |
| 1. Приказ руководства предприятия о разработке проекта комплексной системы защиты информации (КСЗИ). Назначение ответственных за проект. Определение примерных сроков проекта.
 | **2** | **1** |
| 1. Формирование команды разработчиков КСЗИ.
 | **2** | **1** |
| 1. Знакомство с информационной системой и информационными ресурсами предприятия. Составление первого отчета о полученных результатах.
 | **3** | **2** |
| 1. Составление перечня конфиденциальной информации (КИ) предприятия (изучение уже существующего перечня, дополнение, преобразования).
 | **2** | **1** |
| 1. Изучение нормативной документации предприятия.
 | **2** | **1** |
| 1. Изучение журналов регистрации конфиденциальных документов, имеющихся в организации.
 | **3** | **2** |
| 1. Выделение объектов защиты и их категорирование. Составление отчета.
 | **4** | **3** |
| 1. Изучение имеющихся технических средств защиты информации (в том числе на наличие антивирусного ПО)
 | **4** | **3** |
| 1. Проверка технических средств обработки, хранения и передачи информации на наличие средств несанкционированного съема информации и вирусов.
 | **10** | **8** |
| 1. Изучение имеющейся системы охраны периметра организации, системы пожарной безопасности, охранной сигнализации. Изучение прилегающей территории. Выявление пустот в физической защите периметра.
 | **5** | **4** |
| 1. Составление отчета по результатам проверки технических средств, по результатам проведения осмотра периметра. Анализ достаточности уже существующих на предприятии мер защиты.
 | **4** | **3** |
| 1. Разделение персонала организации по уровням доступа к конфиденциальной информации.
 | **5** | **4** |
| 1. Составление новых должностных инструкций, согласование с руководством организации, обоснование.
 | **6** | **5** |
| 1. Анализ достаточности используемых мер защиты. Выявление угроз безопасности, расчет рисков и их ранжирование. Вторичная оценка стоимости проекта.
 | **8** | **7** |
| 1. Составление перечня технических средств защиты, необходимых для дополнения и усовершенствования используемых мер.
 | **4** | **3** |
| 1. Заключение договора на поставку необходимых технических средств, ПО. Установка сроков поставки, монтажа и настройки нового оборудования.
 | **15** | **13** |
| 1. Обучение персонала предприятия работе с новым оборудованием.
 | **4** | **3** |
| 1. Проверка новой систем защиты от несанкционированного проникновения в защищаемое помещение. Искусственная реализация возможных угроз с целью выявления слабых мест в системе защиты.
 | **6** | **5** |
| 1. Составление полного отчета по проделанной работе.
 | **5** | **4** |
| 1. Предоставление проекта директору предприятия.
 | **2** | **1** |
| 1. Возможные доработки и исправления проекта.
 | **2** | **0** |
| Итого  | **98** | **74** |

1. **Структурная схема организации**

Структурная схема организации содержит в себе совокупность должностных лиц, участвующих в проекте по созданию КСЗИ, и выполняемых ими функций в процессе этой деятельности.

В структурную схему входят:

1. Начальник отдела по защите информации
2. Главный инженер по защите информации
3. Начальник службы безопасности
4. Инженер по защите информации
5. Начальник отдела конфиденциального делопроизводства
6. Менеджер по кадрам
7. Сотрудник службы безопасности
8. **Матрица ответственности**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Задачи | Начальник отдела по защите информации | Главный инженер по защите информации | Начальник службы безопасности | Инженер по защите информации | Начальник отдела конфиденциального делопроизводства | Менеджер по кадрам  | Сотрудник службы безопасности |
| 1.Приказ руководства предприятия о разработке проекта комплексной системы защиты информации (КСЗИ). Назначение ответственных за проект. Определение примерных сроков проекта. | x |  | x |  | x |  |  |
| 2. Формирование команды разработчиков КСЗИ. | x |  | x |  | x |  |  |
| 3. Знакомство с информационной системой и информационными ресурсами предприятия. Составление первого отчета о полученных результатах. |  | x |  |  | x | x |  |
| 4. Составление перечня конфиденциальной информации (КИ) предприятия (изучение уже существующего перечня, дополнение, преобразования). | x |  |  |  | x |  |  |
| 5. Изучение нормативной документации предприятия. |  |  |  | x | x |  | x |
| 6. Изучение журналов регистрации конфиденциальных документов, имеющихся в организации. |  |  |  |  | x |  |  |
| 7. Выделение объектов защиты и их категорирование. Составление отчета. | x | x | x |  |  |  |  |
| 8. Изучение имеющихся технических средств защиты информации (в том числе на наличие антивирусного ПО) |  | x |  | x |  |  | x |
| 9. Проверка технических средств обработки, хранения и передачи информации на наличие средств несанкционированного съема информации и вирусов. | x | x |  | x |  |  | x |
| 10. Изучение имеющейся системы охраны периметра организации, системы пожарной безопасности, охранной сигнализации. Изучение прилегающей территории. Выявление пустот в физической защите периметра. |  | x |  | x |  |  | x |
| 11. Составление отчета по результатам проверки технических средств, по результатам проведения осмотра периметра. Анализ достаточности уже существующих на предприятии мер защиты. | x |  | x | x |  |  | x |
| 12. Разделение персонала организации по уровням доступа к конфиденциальной информации. |  |  |  | x |  | x |  |
| 13. Составление новых должностных инструкций, согласование с руководством организации, обоснование. |  |  |  |  | x | x |  |
| 14. Анализ достаточности используемых мер защиты. Выявление угроз безопасности, расчет рисков и их ранжирование. Вторичная оценка стоимости проекта. | x |  | x |  |  |  |  |
| 15. Составление перечня технических средств защиты, необходимых для дополнения и усовершенствования используемых мер. | x | x | x |  |  |  | x |
| 16. Заключение договора на поставку необходимых технических средств, ПО. Установка сроков поставки, монтажа и настройки нового оборудования. |  |  |  | x |  |  | x |
| 17. Обучение персонала предприятия работе с новым оборудованием. |  |  |  | x |  | x | x |
| 18. Проверка новой систем защиты от несанкционированного проникновения в защищаемое помещение. Искусственная реализация возможных угроз с целью выявления слабых мест в системе защиты. | x | x | x | x |  |  | x |
| 19. Составление полного отчета по проделанной работе. | x |  | x |  | x |  |  |
| 20.Предоставление проекта директору предприятия. | x |  | x |  | x |  |  |

1. **Сетевой график и диаграмма Ганта**

Сетевой график представляет собой графическое изобра­жение процесса менеджмента, где все операции, выполнение которых необходимо для достижения конечной цели, показаны в определенной технологической последовательности и взаимозависимости.

При построении сетевого графика используются три основных поня­тия: работа (включая ожидание и зависимость), событие и путь.

Работа– это трудовой процесс, требующий затрат времени и ресур­сов (например, оценка обстановки, анализ информации). На схемах ра­бота изображается в виде сплошной линии со стрелкой. В работу включа­ется процесс ожидания, т.е. процесс, не требующий затрат труда и ресурсов, но требующий затрат времени. Процесс ожидания изобража­ется пунктирной линией со стрелкой с обозначением над ней продолжитель­ности ожидания. Зависимость между двумя или несколькими событиями сви­детельствует об отсутствии необходимости затрат времени и ресурсов, но указывает на наличие связи между работами (начало одной или не­скольких работ зависит от выполнения других), изображается пунктирной линией со стрелкой без обозначения времени.

Событие– это результат выполнения всех работ, входящих в данное событие, позволяющий начинать все выходящие из него работы. На сете­вой матрице событие изображается, как правило, в виде кружка.

Путь – это непрерывная последовательность работ, начиная от исход­ного события и кончая завершающим. Путь, имеющий наибольшую продол­жительность, называется критическим и в матрице обозначается утол­щенной или сдвоенной линией со стрелкой.

# Риски проекта

Последним этапом должно стать выявление всевозможных рисков, с которыми мы можем столкнуться во время реализации проекта, а также определение мер минимизации данных рисков

1. Инвестиционные (экономические).

Основной риск заключается в нехватке денежных средств, материальных ресурсов на реализацию проекта. В этом случае все те мероприятия, которые были осуществлены, не будут приносить нужного результата и можно считать эффективность затраченных средств равной 0.

Также существует достаточно серьезный риск того, что затраты на построение комплексной системы защиты информации окажутся выше, чем выгода от её внедрения на организации.

В целях предотвращения рисков данной группы следует предпринять следующие меры:

* Должна быть произведена профессиональная оценка выгода от внедрения комплексной системы защиты информации
* Стоимость проекта должна быть рассчитана максимально детальна с поправкой в большую сторону.
* Каждый пункт проекта должен быть согласован с коммерческим директором и утвержден генеральным директорам
* Внедряемые меры должны быть экономически оправданы. Выгода от внедрения мер должна превышать затраты на их внедрение.
* Внедряемые меры должны отвечать принципу разумной достаточности. Внедряемые меры должны соответствовать реальным внешним и внутренним угрозам. Не должны быть излишни.
1. Кадровые

Персонал представляет из себя ресурс поведение которого не всегда возможно достаточно точно спрогнозировать даже специалистам. Внедрение комплексной системы защиты информации, а вместе с ней и определенного набора запретительных мер и правил может привести к определенным негативным последствиям в работе персонала.

Данные последствия могут выражаться в следующих формах:

* Сознательное невыполнение обязательных мер защиты
* Многочисленные задержки в работе, связанные со сложностью мер защиты
* Случайные ошибки персонала при работе со средствами защиты

В целях исключения данной группы рисков необходимо при построение комплексной системы защиты информации в обязательном порядке учитывать следующие моменты:

* Ещё до окончательного внедрения должно производиться обучение персонала работе с программно-аппаратными и техническими средствами защиты информации
* Должна быть объяснена необходимость внедрения данных мер с точки зрения, понятной персоналу
* Внедряемые меры по защите информации должны быть просты в эксплуатации
* Внедряемые меры по защите информации должны быть логичны
1. Технические

Та часть рисков, которой зачастую уделяется слишком мало внимания. Суть данной группы рисков заключается в том, что во-первых текущее состояние информационной системы организации должно удовлетворять требования внедряемых мер, во-вторых внедряемые технические меры должны находиться в гармонии с организационными и программно-аппаратными мерами.

Возможные риски:

* Конфликт устанавливаемого программного и аппаратного обеспечения с установленной операционной системой и аппаратной частью
* Сложность в эксплуатации технических и программных средств
* Наличие закладных устройств в устанавливаемых аппаратных средств
* Наличие недекларированных возможностей в инсталлируемых программных средствах

Основные меры предотвращения данной группы рисков:

* Проверка всех поставляемых программных и аппаратных средств
* Выбор надежных поставщиков
* Тщательный выбор необходимых программных и аппаратных средств
1. **Заключение**

Передо мной была поставлена задача создания комплексной системы защиты информации на предприятии «ИТ Энигма». В ходе работы мною было составлено резюме организации, были представлены ограничения, исключения и предложения по мерам защиты, был приведен пример расчета рисков. В итоге работы была составлена структурная схема организации и матрица ответственности.