Министерство образования Российской Федерации

Федеральное агентство по делам образования и науки

Южно-Уральский Государственный Университет

Факультет Экономики и Предпринимательства

Кафедра Информационной безопасности

**Курсовая работа**

по дисциплине «Информационная безопасность сложных систем»

на тему: «Создание комплексной системы защиты информации» (Интернет-провайдер)

Челябинск

2007**Оглавление**

[Описание информационной системы организации 5](#_Toc188623631)

[Состояние фактической защищённости организации 6](#_Toc188623632)

[Резюме проекта 8](#_Toc188623633)

[Требования к защищённости информации 8](#_Toc188623634)

[Объекты поставки 10](#_Toc188623635)

[Структура разбиения работ 12](#_Toc188623636)

[Расчетная стоимость предлагаемых мер 16](#_Toc188623637)

[Оценка эффективности и целесообразности внедряемой комплексной системы защиты информации 18](#_Toc188623638)

[Диаграмма Ганта 19](#_Toc188623639)

[Сетевой график 20](#_Toc188623640)

[Риски проекта 21](#_Toc188623641)

[Заключение 24](#_Toc188623642)

[Список использованной литературы 25](#_Toc188623643)

[Приложение 1. Диаграмма Ганта 26](#_Toc188623644)

**Введение**

Создание системы защиты информации для организаций, занимающихся предоставлением телематических услуг, является обязательной составляющей деятельности организации Интернет-провайдера.

Данная необходимость обусловлена тем, что подобные организации обрабатывают большой объем конфиденциальных сведений, в том числе персональные данные, защита которых обязательна по требованиям законодательства.

Жесткая конкуренция на рынке приводит к тому, что конфиденциальная информация, которой обладает организация, может дать значительное конкурентное преимущество.

Также комплексная система защиты информации позволит обеспечить бесперебойное функционирование сервисов, предотвратить прямые материальные потери от утечки или утраты конфиденциальной информации, а также предотвратить возможный ущерб репутации компании.

Для того, чтобы определить целесообразность создания КСЗИ, зону и глубину её охвата следует провести детальный анализ организации, включающий:

* Анализ деятельности предприятия
* Положение организации на рынке
* Выявление конфиденциальной информации и защищаемых ресурсов
* Анализ угроз, уязвимостей и потенциального ущерба от реализации угрозы

На основе полученной информации о деятельности организации и уязвимых местах в действующей системе защиты необходимо составить техническое задание на создание комплексной системы защиты информации.

Исходя из существующего технического задания, следует определить практические меры для его реализации. Совокупность этих мер составит проект внедрения комплексной системы защиты информации.

В ходе выполнения данной работы необходимо

* Выявить требования, предъявляемые к создаваемой комплексной системе защиты информации
* Составить детальный список мероприятий, необходимых для внедрения комплексной системы защиты информации
* Назначит ответственных за проводимые мероприятия
* Произвести оценку затрат ресурсов на внедряемые мероприятия
* Оценить эффективность проводимых мероприятий

# **Описание информационной системы организации**

АС организации состоит из 10 автоматизированных рабочих мест и 6 серверов.

* 1 АРМ представляет собой компьютер Mac mini с установленной ОС MAC OS.
* На трёх АРМ установлена операционная система на базе Linux.
* На всех остальных установлена ОС Windows XP.
* На всех АРМ хранится и обрабатывается конфиденциальная информация.
* На серверах установлена операционная система на базе Linux
* На АРМ менеджеров установлено следующее ПО:
	+ ОС на базе Windows
	+ Офисное программное обеспечение
	+ ПО для работы в сети Интернет: почтовый клиент, браузер
	+ Антивирусное ПО
	+ Специализированные программы: Дельфин, Дубль-ГИС
* На АРМ консультантов технической поддержки установлено следующее ПО:
	+ ОС на базе Linux
	+ Офисное программное обеспечение

ПО для работы в сети Интернет: почтовый клиент, браузер

**Состояние фактической защищённости организации**

* Перечень конфиденциальной информации существует и утвержден
* Все сотрудники, при приёме на работу подписывают обязательство о неразглашении конфиденциальной информации
* Во всех помещениях установлены датчики охранной и пожарной сигнализации. В нерабочее время помещения сдаются под охрану
* Охрана осуществляется частным охранным агентством
* Существует перечень лиц, имеющих доступ в серверную комнату
* Серверная комната постоянно закрыта, кроме тех случаев, когда сотрудникам, имеющим соответствующие права доступа, необходимо производить определённые работы
* Права доступа к локальным и сетевым ресурсам АРМ ограничиваются штатными средствами операционной системы
* Нет ответственного за разграничение доступа к локальным и сетевым ресурсам АРМ. Разграничением доступа занимается пользователь АРМ.
* Доступ к ресурсам на сервере ограничивается штатными средствами операционной системы
* Ответственным за разграничение доступа к ресурсам на сервере является старший системный администратор
* Назначение прав пользователей производится по указанию технического директора либо заместителя директора в соответствии с должностными обязанностями сотрудника
* Каждый компьютер подключен через источник бесперебойного питания, позволяющий обеспечить непрерывную работу в течение 10-15 минут при отсутствии электричества
* В серверной комнате установлено несколько источников бесперебойного питания высокой емкости, а также дизельная миниэлектростанция
* Доступ в Интернет осуществляется через прокси-сервер
* Правила обращения с конфиденциальной информацией отсутствуют
* Фильтрация содержания электронной почты, просматриваемых сайтов не осуществляется
* Хранение договоров с клиентами осуществляется в шкафу.
* Разграничения доступа помещения в зависимости от отделов нет.

#

# **Резюме проекта**

На основании проведенного анализа фактической защищенности необходимо составить перечень требований к создаваемой комплексной системе защиты информации. Данные требования должны соответствовать реальному состоянию защищенности информации в организации. Требования должны быть оформлены в виде Технического задания на создание комплексной системы защиты информации.

##

## **Требования к защищённости информации**

**Организационно-правовая составляющая**

Организационные мероприятия являются одной из важнейших составляющих комплексной системы защиты информации в организации.

1. Перечень конфиденциальных сведений должен отвечать реальному состоянию организации и требованиям законодательства РФ
2. Должен быть обеспечен полный пакет документов, связанных с обеспечением информационной безопасности в организации
3. Организационными мерами обеспечить конфиденциальность информации при проведении конфиденциальных совещаний и переговоров
4. Должен быть подготовлен пакет документов, регламентирующих правила обращения с конфиденциальной информацией
5. Разграничение прав пользователей на доступ как к локальным, так и к сетевым ресурсам должно быть контролируемым и документируемым процессом.

**Инженерно-техническая составляющая**

1. Должны применяться технические средства контроля доступа в помещения
2. Для защиты серверной комнаты должны применяться дополнительные технические средства контроля доступа
3. Должны применяться технические средства защиты акусто-речевой информации при проведении конфиденциальных совещаний и переговоров в том случае, если невозможно обеспечить конфиденциальность переговоров с помощью организационных мер.
4. С помощью технических средств должна обеспечиваться защита от утечки конфиденциальной информации по каналу ПЭМИН
5. Должна быть обеспечена бесперебойная работа ПК сотрудников в случае отключения электричества не менее, чем на 10 минут
6. Должна обеспечиваться бесперебойная работа основного оборудования и технических средств, установленных в серверной на весь срок отсутствия основного энергоснабжения

**Программно-аппаратная составляющая**

1. Содержимое просматриваемых веб-сайтов должно отвечать следующим требованиям:
	1. Не должно содержать материалов, запрещённых законодательством Российской Федерации
	2. Должно быть безопасным (не содержать вирусы, вредоносные скрипты)
	3. Не должно содержать материалы, не относящиеся к рабочему процессу
2. Обмен информацией с помощью различных программных средств не должен наносить ущерб конфиденциальности, целостности, доступности информации
3. С помощью программно-аппаратных средств должна обеспечиваться защита от НСД к конфиденциальной информации, хранящейся на АРМ сотрудников и на сервере.

 **Объекты поставки**

Организационно-правовая подсистема:

* Перечень конфиденциальных сведений
* Перечень конфиденциальных документов
* Политика безопасности
* Техническое задание
* Положение о конфиденциальном документообороте
* Инструкции о порядке обращения с конфиденциальной информацией

Инженерно-техническая подсистема:

* Металлическая дверь типа «Сейф-дверь»
* Датчики пожарной сигнализации
* Датчики охранной сигнализации
* Видеокамеры цветные с системой ночного видения
* Мониторы видеонаблюдения 10”
* Видеорегистратор с объемом диска для хранения видеозаписи не менее 5 суток
* Генератор виброакустического шума Соната АВ
* Виброизлучатели
* Акустоизлучатели
* Устройство блокирования сотовых телефонов
* Источники бесперебойного питания
* Генератор электромагнитного шума
* Считыватели пластиковых карт
* Металлические решетки
* Дверь с тамбуром

Программно-аппаратная подсистема:

* Программный комплекс для автоматизации документооборота
* Программно-аппаратный комплекс для защиты от НСД «SecretNet 5.0»
* Межсетевой экран «Континент»
* Сервер

# **Структура разбиения работ**

Данные мероприятия реализуются путем выполнения ряда последовательных работ, которые представлены в разделе «Структура разбиения работ».

АМ

Создание Комплексной системы защиты информации

**4.** **Структурная схема организации**

АМ.01.2

АМ.01.1.3

АМ.01.1.2

АМ.01.1.1

АМ.01.1

Обучение сотрудников

Разработка положений, касающихся отдельных аспектов ИБ

Разработка инструкций о порядке обращения с КИ

Разработка положения о конфиденциальном документообороте

Разработка основных нормативно-правовых документов

АМ.03.6

АМ.03.5

АМ.03.4

АМ.03.3

АМ.03.2

АМ.03.1

Внедрение парольной политики

Разграничение прав пользователей

Создание резервных серверов

Установка и настройка межсетевого экрана

Установка и настройка программно-аппаратных средств контроля доступа

Создание автоматизированной системы документооборота

Организация защиты от акустического съема информации

Настройка и запуск в эксплуатацию системы видеонаблюдения

Закупка мониторов

Закупка видеорегистраторов

Закупка видеокамер

Организация видеонаблюдения

Установка системы пожарной сигнализации

Установка системы охранной сигнализации

АМ.02.4.2

АМ.02.4.1

АМ.02.4

АМ.02.3.4

АМ.02.3.3

АМ.02.3.2

АМ.02.3.1

АМ.02.3

АМ.02.2

АМ.02.1

Организация тамбура

Установка средств виброакустического зашумления

АМ.03

АМ.01

АМ.02

Организационно-правовая система

Инженерно-техническая система

Программно-аппаратная система

АМ.02.8

АМ.02.7.2

АМ.02.7.1

АМ.02.7

АМ.02.6.2

АМ.02.6.1

АМ.02.6

Установка систем контроля доступа в помещения

Монтаж ограждения

Установка считывателя магнитных карт

Установка двери типа «Сейф-дверь»

Установка систем контроля доступа в здание

АМ.02.5.2

АМ.02.5.1

АМ.02.5

АМ.02.4.3

Организация поста охраны

Установка систем контроля доступа на территорию

Установка систем блокирования сотовых телефонов

Установка решеток на окнах

Установка систем электромагнитного зашумления

Установка считывателя магнитных карт

Структурная схема организации позволяет выявить иерархические связи между сотрудниками организации. В дальнейшем данная схема позволяет составить матрицу ответственности, из которой можно определить, какой сотрудник, за какие мероприятия отвечает.

Коммерческий директор

Генеральный директор

Менеджер проекта (начальник отдела ИБ)

Технический директор

Администратор

Документовед

Специалист отдела кадров

Специалист по ЗИ

Инженер по ЗИ

Техник по ЗИ

Монтажник ЛВС

ВР.01

ВР.01.1

ВР.01.1.1

ВР.01.1.2

ВР.01.2

ВР.01.3

ВР.01.2.1

ВР.01.2.2

ВР.01.2.3

ВР.01.3.1

ВР.01.3.2

**Матрица ответственности**

Матрица ответственности позволяет определить конкретных исполнителей того или иного мероприятия.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  Исполнители Работы | ВР.01 | ВР.01.1 | ВР.01.1.1 | ВР.01.1.2 | ВР.01.2 | ВР.01.2.1 | ВР.01.2.2 | ВР.01.2.3 | ВР.01.3 | ВР.01.3.1 | ВР.01.3.2 |
| 1 | АМ.01.1 |  |  |  |  |  | х |  |  |  | х |  |
| 2 | АМ.01.1.1 |  |  |  |  |  | х |  |  |  | х |  |
| 3 | АМ.01.1.2 |  |  |  |  |  | х |  |  |  | х |  |
| 4 | АМ.01.1.3 |  |  |  |  |  | х |  |  |  | х |  |
| 5 | АМ.01.2 | х |  |  |  | х |  |  |  | х |  | х |
| 6 | АМ.02.1 |  |  |  |  |  |  | х | х |  |  |  |
| 7 | АМ.02.2 |  |  |  |  |  |  | х | х |  |  |  |
| 8 | АМ.02.3 |  |  | х |  | х | х | х |  | х |  |  |
| 9 | АМ.02.3.1 |  |  |  |  | х | х |  |  | х |  |  |
| 10 | АМ.02.3.2 |  |  |  |  | х | х |  |  | х |  |  |
| 11 | АМ.02.3.3 |  |  |  |  | х | х |  |  | х |  |  |
| 12 | АМ.02.3.4 |  |  | х |  |  | х | х |  |  |  |  |
| 13 | АМ.02.4 |  |  |  |  | х | х | х | х |  |  |  |
| 14 | АМ.02.4.1 |  |  |  |  |  | х | х | х |  |  |  |
| 15 | АМ.02.4.2 |  |  |  |  |  |  | х | х |  |  |  |
| 16 | АМ.02.4.3 |  |  |  |  | х | х |  |  |  |  |  |
| 17 | АМ.02.5 | х | х | х | х |  |  |  | х | х | х | х |
| 18 | АМ.02.5.1 |  |  | х | х |  |  |  | х |  |  |  |
| 19 | АМ.02.5.2 | х | х |  |  |  |  |  |  | х | х | х |
| 20 | АМ.02.6 |  |  |  |  |  |  | х | х |  |  |  |
| 21 | АМ.02.6.1 |  |  |  |  |  |  | х | х |  |  |  |
| 22 | АМ.02.6.2 |  |  |  |  |  | х | х | х |  |  |  |
| 23 | АМ.02.7 |  |  |  |  |  |  | х | х |  |  |  |
| 24 | АМ.02.7.1 |  |  |  |  |  | х | х | х |  |  |  |
| 25 | АМ.02.7.2 |  |  |  |  |  |  | х | х |  |  |  |
| 26 | АМ.02.8 |  |  |  |  |  |  |  | х |  |  |  |
| 27 | АМ.03.1 |  |  | х |  | х | х |  |  |  |  |  |
| 28 | АМ.03.2 |  |  | х |  | х | х |  |  |  |  |  |
| 29 | АМ.03.3 |  |  | х |  |  | х |  |  |  |  |  |
| 30 | АМ.03.4 |  |  | х |  |  | х |  |  |  |  |  |
| 31 | АМ.03.5 |  |  | х |  |  | х |  |  |  |  |  |
| 32 | АМ.03.6 |  |  | х |  |  | х |  |  |  |  |  |

# **Расчетная стоимость предлагаемых мер**

|  |  |
| --- | --- |
| **Мероприятия по защите** | **Стоимость** |
| Установка системы охранной сигнализации | 20 000 |
| Установка системы пожарной сигнализации | 15 000 |
| Организация видеонаблюдения |  |
| Закупка видеокамер | 56 000 |
| Закупка видеорегистраторов | 36 000 |
| Закупка мониторов | 18 000 |
| Настройка и запуск в эксплуатацию системы видеонаблюдения | 5 000 |
| Организация защиты от акустического съема информации |  |
| Установка систем виброакустического зашумления | 50 000 |
| Организация тамбура в помещение | 3 000 |
| Установка систем блокирования сотовых телефонов | 22 000 |
| Установка систем контроля доступа на территорию |  |
| Монтаж ограждения | 40 000 |
| Организация поста охраны | 36 000 |
| Установка системы контроля доступа в здание |  |
| Установка двери типа «Сейф-дверь» | 15 000 |
| Установка считывателя магнитных карт | 5 000 |
| Установка системы контроля доступа в помещения |  |
| Установка считывателя магнитных карт | 50 000 |
| Установка решеток на окнах | 10 000 |
| Установка систем электромагнитного зашумления | 20 000 |
| Создание автоматизированной системы документооборота | 30 000 |
| Установка и настройка программно-аппаратных средств контроля доступа | 50 000 |
| Установка и настройка межсетевого экрана | 100 000 |
| Создание резервных серверов | 60 000 |
| Разграничение прав пользователей | 2 000 |
| Внедрение парольной политики | 1 000 |
| Разработка положения о конфиденциальном документообороте | 3 000 |
| Разработка инструкций о порядке обращения с КИ | 3 000 |
| Разработка положений, касающихся отдельных аспектов обеспечения ИБ | 5 000 |
| Обучение сотрудников | 20 000 |
| **Итоговая сумма на создание КСЗИ** | **675 000** |

# **Оценка эффективности и целесообразности внедряемой комплексной системы защиты информации**

Итоговая сумма на создание комплексной системы защиты информации получилась равной 675 000 рублей.

Ценность информации, обрабатываемой в организации, исчисляется несколькими миллионами рублей. Помимо прямого финансового ущерба потеря конфиденциальности или утрата данной информации может нанести и косвенный ущерб, связанный с ущербом репутации компании. Данный ущерб выражается в ещё большей сумме – порядка 20 миллионов рублей.

При данных расчетах учитывалось ежемесячное число подключаемых клиентов компании, стоимость реализации рекламной кампании, а также ущерб от блокирования работы информационной системы компании.

**Диаграмма Ганта**

Диаграмма Ганта представляет собой отрезки (графические плашки), размещенные на горизонтальной шкале времени. Каждый отрезок соответствует отдельной задаче или подзадаче. Задачи и подзадачи, составляющие план, размещаются по вертикали. Начало, конец и длина отрезка на шкале времени соответствуют началу, концу и длительности задачи.

Диаграмма Ганта позволяет определить сроки окончания работы, установить те моменты времени, в которые определенные сотрудники находились без работы или наоборот были загружены сверх меры.

Диаграмма Ганта находится в Приложении 1.

# **Сетевой график**

**Таблица параметров проекта**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Код работы | Ожидаемая продолжительность | Срок начала | Срок окончания | Резерв |
| Раннее | Позднее | Раннее | Позднее |
| **1-2** | **45** | **0** | **0** | **45** | **45** | **0** |
| 1-3 | 7 | 0 | 73 | 7 | 80 | 73 |
| 1-4 | 14 | 0 | 66 | 14 | 80 | 66 |
| 1-5 | 14 | 0 | 50 | 14 | 64 | 50 |
| 1-6 | 14 | 0 | 66 | 14 | 80 | 66 |
| **2-7** | **14** | **45** | **45** | **59** | **59** | **0** |
| 5-8 | 5 | 14 | 75 | 19 | 69 | 61 |
| 5-9 | 5 | 14 | 75 | 19 | 80 | 61 |
| 5-10 | 5 | 14 | 64 | 19 | 80 | 50 |
| **7-11** | **3** | **59** | **59** | **62** | **62** | **0** |
| 8-12 | 5 | 19 | 69 | 24 | 74 | 50 |
| **11-13** | **1** | **62** | **62** | **63** | **63** | **0** |
| 11-14 | 1 | 62 | 74 | 63 | 75 | 12 |
| 11-15 | 5 | 62 | 75 | 67 | 80 | 13 |
| 12-16 | 1 | 24 | 74 | 25 | 78 | 50 |
| 12-17 | 2 | 24 | 78 | 26 | 80 | 54 |
| 12-18 | 6 | 24 | 74 | 30 | 80 | 50 |
| **13-19** | **5** | **63** | **63** | **68** | **68** | **0** |
| 14-20 | 5 | 63 | 75 | 68 | 80 | 12 |
| 16-21 | 1 | 25 | 79 | 25 | 80 | 54 |
| **19-22** | **5** | **68** | **68** | **73** | **73** | **0** |
| **22-23** | **7** | **73** | **73** | **80** | **80** | **0** |

# **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

# **Заключение**

В ходе выполнения работы мы выяснили, какие мероприятия необходимы для построения комплексной системы защиты информации в организации. С помощью составленной структуры организации была рассчитана матрица ответственности, которая позволяет выявить ответственных за то или иное мероприятие.

Благодаря подробному плану мероприятий можно оценить общую итоговую стоимость построения комплексной системы защиты информации.

Несмотря на достаточно высокую стоимость создания комплексной системы защиты информации (~700 000 рублей), данные мероприятия полностью окупают себя в виду высокой стоимости защищаемой информации.

Для того, чтобы обезопасить проект от неожиданностей, был произведен анализ рисков проекта, а также мер по их минимизации.

Итогом проекта является создание комплексной системы защиты информации в организации.

# **Список использованной литературы**

Способы и средства предотвращения утечки информации по техническим каналам М: ЗАО НПЦ НЕЛК, 2003 г.

Торокин А. А. Инженерно- техническая защита информации: Учеб. пособие для вузов/А. А. Торокин. - М.: Гелиос АРВ, 2005.

Федеральный закон Об информации, информационных технологиях и защите информации (от 20.02.95 г. № 24-ФЗ). М.: Эксмо, - 1995.

Федеральный закон О коммерческой тайне (от 25.07.2004 г. № 98-ФЗ). М.: Эксмо, - 2005.

# **Приложение 1. Диаграмма Ганта**

