**АННОТАЦИЯ**

Жоможаева Е.Г.. Разработка проекта КСЗИ

Администрации города Миасса. –

Челябинск: ЮУрГУ,

Кафедра Информационная безопасность, 2008

Список литературы – 15 наименования.

В курсовом проекте рассмотрена разработка проекта комплексной системы защиты информации на примере Администрации города Миасса. Проанализирована характеристика объекта защиты; построена модель бизнес-процессов с целью выявления конфиденциальной информации, составлен «Перечень сведений конфиденциального характера», выявлены объекты защиты, угрозы, уязвимости и рассчитаны риск для ключевых объектов защиты, построена модели злоумышленника; проанализирована степень защищенности организации по каждому из видов защиты информации (ЗИ) (правовая ЗИ, организационная ЗИ, программно-аппаратная ЗИ, инженерно-физическая ЗИ) и предложены меры по обеспечению защищенности организации.

**Содержание:**

1. Введение 3
2. Паспорт предприятия. 5
3. Описание модели бизнес-процессов 9
4. Задачи построения КСЗИ 10
5. Этапы построения КСЗИ 11
6. Расчет информационных рисков 13
7. Разработка ПИБ 19
8. Заключение 20
9. Источники 21
10. Приложения

**Введение.**

С каждым годом увеличивается количество информации, растет ее спрос, а значит и растет ее ценность, связи с этим возрастают требования по ее защите. Так же быстрыми темпами совершенствуются компьютерные технологии. Из-за ежегодного обновления компьютерных технологий возникают новые угрозы для информации. Следовательно, возрастет необходимость ее защиты. Для того чтобы защита была полной необходимо прорабатывать ее комплексно.

Утечка любой информации может отразиться на деятельности организации. Особую роль играет конфиденциальная информация, потеря корой может повлечь большие изменения в самой организации и материальные потери. Так как Администрация г. Миасса является управленческим органом, то потеря конфиденциальной информации может повлечь потери не только для самой Администрации, как организации, так и для всего города в целом. Поэтому мероприятия по защите информации в данное время очень актуальны и важны.

Для обеспечения полноценной защиты конфиденциальной информации необходимо проводить комплексный анализ каналов утечки, каналов и методов несанкционированного воздействия на информацию.

Целью своей курсовой работы я избрала разработку проекта КСЗИ на примере Администрации города Миасса..

Задачи, которые я поставила перед собой:

1. Проанализировать общую характеристику объекта защиты, оформленную в виде «Паспорта предприятия»;
2. Построить модель бизнес-процессов с целью выявления конфиденциальной информации;
3. Составить «Перечень сведений конфиденциального характера»;
4. Выявить объекты защиты, оформленные в виде «Списка объектов, подлежащих защите»;
5. Выявить угрозы, уязвимости и произвести расчет рисков для ключевых объектов защиты;
6. Построить модель злоумышленника;
7. Проанализировать степень защищенности объектов защиты по каждому из видов защиты информации (ЗИ) (правовая ЗИ, организационная ЗИ, программно-аппаратная ЗИ, инженерно-физическая ЗИ, криптографическая ЗИ);

**Паспорт предприятия.**

Здание Администрации находится в районе. По адресу г. Миасс, пр.Автозаводцев,55. Здание Администрации является трехэтажным. Имеет свой хозяйственный двор для служебного автотранспорта. Перед зданием имеется автопарковка. Вход людей в здание осуществляется через контрольно-про­пускной пункт, находящемся на 1-ом этаже здания.

Доступ имеет свои разграничения:

— в Отдел, занимающийся вопросами работы с вопросами и просьбами населения, имеют доступ все посетители. Отдел находится на первом этаже здания.

— В отделы и помещения, находящиеся на втором этаже здания, где находиться конфиденциальная информация допуск осуществляемся только по пропускам.

— Во все остальные помещения и отделы имеют доступ лишь служащие и клиенты по записи,

— Доступ в кабинет Главы города в его отсутствие запрещен.

Границе КЗ Администрации является забор, ограничивающий периметр здания и хоз. двора..

Электропитание здания осуществляется от трансформаторной подстанции, которая расположена на неконтролируемой территории и обслуживается сторонней организацией.

Здание окружено жилыми домами (5- этажными).

В состав ВТСС входят:

— система кондиционирования (по одному в каждом кабинете);

— телефонный аппарат (в каждом кабинете, телефонная связь осуществляется через общую АТС здания, кабели АТС выходят за пределы КЗ) . В каждом отделе по 2.

— компьютер ( на каждом рабочем месте, состав: системный блок, монитор, мышь, клавиатура, 2 динамика)

— принтер (в каждом отделе по 1 штуке).

— телевизор (1шт. в кабинете Главы города).

В Администрации в каждом кабинете по 1-3 окна, в зависимости от площади кабинета. Все окна – тройной евростеклопакет. На окнах установлены жалюзи. Окна с одной стороны здания выходят на хоз. двор., остальные на шумные улицы

Количество стояков отопления соответствует количеству окон. Трубы системы отопления проходят по всем этажам, заканчиваются в бойлерной(подвальное помещение здания).

Стены, потолок – железобетонные плиты толщиной 400 мм, отделаны гипсокартонном толщиной10мм, пол – железобетонные плиты толщиной 400 мм, покрытые паркетом (отделы) и ковролином (кабинет Главы города).

Количество дверей соответствует количеству кабинетов в здании.

Дверь входа в здание – железная укрепленная.

Требования к монтажу кабельной проводки – скрытый монтаж.

Генераторы вибро-акустического зашумления не установлены.

Генераторы электромагнитного шума не установлены.

Направления деятельности Администрации:

— юридический отдел;

— комитет по управлению Машгородка;

— отдел муниципального обслуживания;

— вопросами безопасности;

— проблемами строительства;

— вопросы ЗАГСа;

— вопросами коммунального хозяйства, распределения жилья;

— вопросы гуманитарного развития ;

— вопросы экономического развития;

— вопросами кадрового развития;

— вопросами хозяйственного обслуживания;

На предприятии отсутствуют сведения, составляющие государственную тайну, но ведется работа с коммерческой и служебной тайной. Существует ряд нормативно- правовых актов регламентирующих правила пользования этими сведениями.

В Администрации существует своя локальная сеть, доступ к которой имеют только служащие Администрации. В большинстве случаев имеется доступ лишь к ограниченному числу сайтов этой сети, необходимых в ходе трудовой деятельности. Информация о каждом выходе в сеть фиксируется системным администратором. Это также относится к сети Интернет.

Основными объектами защиты являются:

— АРМ сотрудников;

— сервер локальной сети;

— конфиденциальная информация (документы);

— кабинет Главы города;

— зал проведения совещаний;

— кабинеты с конфиденциальной документацией.

В Администрации разработана часть мер по защите информации:

— заключен договор об охране помещения и территории;

— разработан график работы и посещения населения;

— разработан режим и правила противопожарной безопасности;

— режим видеонаблюдения этажей;

— разработаны должностные инструкции служащих, разграничивающие их права и обязанности ;

—дополнительные соглашения к трудовым договорам сотрудников о неразглашении ими конфиденциальной информации, регламентирующие ответственность в области защиты информации;

— инструкции по охране периметра, по эксплуатации системы охранной сигнализации и видеонаблюдения;

— положение о конфиденциальном документообороте;

— описание технологического процесса обработки КИ;

­— установлена антивирусная системы защиты на АРМ;

— разграничен доступ к АРМ паролями.

## Описание модели бизнес-процессов.

Модель бизнес-процесса Администрации города Миасса максимально подробно описан в Приложении №1, с помощью построения модели BPwin.

Проанализировав структуру Администрации можно выделить, что она имеет очень обширную сферу деятельности. Потому, что состоит из множества отделов. В каждом отделе рассматриваются различные вопросы по обеспечению жизнедеятельности города. Каждый отдел несет ответственность за свои действия.

Деятельность Администрации является очень важной, потому как это муниципальные орган управления города.

**Задачи построения КСЗИ.**

После анализа имеющихся данных можно выделить ряд задач необходимых для построения КСЗИ:

— дополнение имеющихся мер защиты, внедрение и организацию;

— составить комплекс организационных мероприятий;

—проработать перечень программно-аппаратных и инженерно-технических мер;

— необходимо составить перечень конфиденциальной информации;

— составляется перечень объектов защиты;

— определить перечень угроз для этих объектов;

— рассчитать информационные риски.

Рассмотрев состав информационных ресурсов предприятия, определяем состав конфиденциальной информации:

— Сведения, составляющие коммерческую тайну;

— Сведения, содержащие персональные данные.

Получаем перечень сведений, составляющих конфиденциальную информацию (Приложение №2);

Также необходимо определить местоположение защищаемой информации на предприятии. Для этого составляется перечень объектов защиты (Приложение №5), включающий структурную графическую схему второго этажа в здании Администрации (Приложение №6), где проходит основной поток конфиденциальной информации.

**Этапы построения КСЗИ.**

Для создания комплексной системы защиты информации на предприятии необходимо провести ряд мероприятий:

Эти мероприятия может проводить как специально приглашённая фирма- исполнитель, так и служба безопасности предприятия (если она имеет лицензию на осуществление этой деятельности).

1.Стартовый (начальный).

— Получение согласия высшего руководства на создание КСЗИ.

— Разработка плана работ по созданию КСЗИ.

— Формирование команды по созданию КСЗИ.

В результате проведения этого этапа должны появиться следующие документы:

— Приказ о создании КСЗИ,

— план работ по созданию КСЗИ,

— приказ о формировании команды,

— приказ о проведении обследования предприятия.

2. Этап предпроектного обследования.

На этом этапе проводится обследование (аудит) предприятия.

— Инвентаризация объектов информатизации и персонала.

— Выявление информационных потоков.

— Моделирование бизнес-процессов.

— Разработка отчёта, в который должны входить: объекты защиты с точки зрения угроз, модели злоумышленников, ответственные за объекты информатизации, расчёт рисков, ранжирование рисков.

— Разработка технического задания на проектирование КСЗИ. В него входят ключевые объекты защиты, меры и средства защиты, требования по защите.

3. Проектирование.

— Создание системного проекта.

— Создание “Политики безопасности”.

— Проведение работ по созданию КСЗИ (технический проект с опорой на ресурсы, «Технический проект на создание КСЗИ» представляет собой комплект документов, в который входит часть документов разработанных на предыдущих этапах и ряд новых документов, в которых описано, как именно будет создаваться, эксплуатироваться и, в случае необходимости, модернизироваться КСЗИ).

— Создание рабочего проекта.

4. Внедрение

На этом этапе создаётся пакет документов «Эксплуатационная документация на КСЗИ», который включает:

— Инструкции эксплуатации КСЗИ и её элементов;

— Процедуры регламентного обслуживания КСЗИ;

— Правила и положения по проведению тестирования и анализа работы КСЗИ.

На этом этапе проводится все пусконаладочные работы, обучает и инструктирует персонал предприятия правилам и режимам эксплуатации КСЗИ.  
После реализации этого этапа внедренная КСЗИ готова к последующему испытанию. В процессе испытаний выполняются тестовые задания и контролируются полученные результаты, которые и являются индикатором работоспособности спроектированной КСЗИ. По результату испытания КСЗИ делается вывод относительно возможности представления КСЗИ на государственную экспертизу.

**Расчет информационных рисков.**

**Критичность ресурса** (D) – степень значимости ресурса. Отражает влияние реализации угрозы на работу информационной системы.

**Критичность реализации угрозы** (ER) – степень влияния реализации угрозы на ресурс. Задается в %.

**Вероятность реализации угрозы** через данную уязвимость в течении года (P(v)) – степень возможности реализации угрозы через данную уязвимость в тех или иных условиях, указывается в %.

1. Объект защиты – автоматизированное рабочее место **(АРМ) сотрудника**.

Критерий критичности (D) равен 5000 рублей.

*Таблица угроз и уязвимостей.*

|  |  |
| --- | --- |
| *Угроза* | *Уязвимости* |
| 1.Физический доступ нарушителя к АРМ | 1. Отсутствие системы контроля доступа служащих к чужим АРМам |
| 2.Отсутствие системы видеонаблюдения  на предприятии |
| 3. Несогласованность в системе охраны периметра задания |
| 2.Разглашение КИ, хранящейся на АРМ | 1.Отсутствие соглашения о неразглашении между Администрацией и служащими. |
| 2.Нечеткое распределение ответственности между служащими |
| 3.Разрушение КИ при помощи специальных программ и вирусов | 1.Отсутствие или некорректная работа антивирусного ПО |
| 2.Отсутствие ограничения доступа пользователей к внешней сети |

*Таблица вероятности реализации данной угрозы через уязвимость в течении года(P(V)) и критичности реализации угрозы (ER).*

|  |  |  |
| --- | --- | --- |
| *Угроза/уязвимость* | *P(V), %* | *ER,%* |
| 1/1 | 50 | 50 |
| 1/2 | 30 | 50 |
| 1/3 | 10 | 40 |
| 2/1 | 30 | 40 |
| 2/2 | 50 | 40 |
| 3/1 | 10 | 90 |
| 3/2 | 20 | 60 |

*Таблица уровня угрозы по определённой уязвимости (Th) и по уровню угроз по всем уязвимостям (CTh).*

|  |  |  |
| --- | --- | --- |
| *Угроза/уязвимость* | *Th* | *CTh* |
| 1/1 | 0,25 | 0,975 |
| 1/2 | 0,15 |
| 1/3 | 0,04 |
| 2/1 | 0,12 | 0,296 |
| 2/2 | 0,2 |
| 3/1 | 0,09 | 0,199 |
| 3/2 | 0,12 |

Th=P(V)/100\*ER/100

CTh=1-П(1-Th)

Рассчитаем общий уровень угроз по ресурсу:

CThR=1-П(1-CTh)=1-0,025\*0,04\*0,801=0,986

Рассчитаем риск по ресурсу:

R= CThR\*D=0,986\*7500=**7395 (руб).**

Объект защиты – **сервер локальной сети.**

Критерий критичности (D) равен 15000 рублей.

*Таблица угроз и уязвимостей.*

|  |  |
| --- | --- |
| *Угроза* | *Уязвимости* |
| 1.Физический доступ нарушителя к серверу | 1.Неорганизованность контрольно-пропускного режима на предприятии |
| 2.Отсутствие видеонаблюдения |
| 2.Разглашение КИ, хранящейся на сервере | 1.Отсутствие соглашения о нераспространении КИ |
| 2. Нечеткое распределение ответственности между сотрудниками предприятия |

*Таблица вероятности реализации данной угрозы через уязвимость в течении года(P(V) и критичности реализации угрозы (ER).*

|  |  |  |
| --- | --- | --- |
| *Угроза/уязвимость* | *P(V), %* | *ER,%* |
| 1/1 | 70 | 80 |
| 1/2 | 40 | 60 |
| 2/1 | 30 | 30 |
| 2/2 | 70 | 50 |

*Таблица уровня угрозы по определённой уязвимости (Th) и по уровню угроз по всем уязвимостям (CTh).*

|  |  |  |
| --- | --- | --- |
| *Угроза/уязвимость* | *Th* | *CTh* |
| 1/1 | 0,56 | 0,666 |
| 1/2 | 0,24 |
| 2/1 | 0,09 | 0,408 |
| 2/2 | 0,35 |

Th=P(V)/100\*ER/100

CTh=1-П(1-Th)

Рассчитаем общий уровень угроз по ресурсу:

CThR=1-П(1-CTh)=1-0,344\*0,592=0,796

Рассчитаем риск по ресурсу:

R=CTh\*D=0,796\*15000=**11940 (руб).**

1. Объект защиты – **Конфиденциальная документация.**

Критерий критичности (D) равен 3000 рублей.

*Таблица угроз и уязвимостей.*

|  |  |
| --- | --- |
| *Угроза* | *Уязвимости* |
| 1.Физический доступ нарушителя к документам | 1.Неорганизованность контрольно-пропускного режима на предприятии |
| 2.Отсутствие видеонаблюдения |
| 2.Разглашение КИ, используемой в документах, вынос документов за пределы КЗ | 1.Отсутствие соглашения о неразглашении КИ |
| 2. Нечеткое распределение ответственности за документы между сотрудниками предприятия |
| 3.Несанкционированное копирование, печать и размножение КД | 1. Нечеткая организация конфиденциального документооборота |
| 2. Неконтролируемый доступ сотрудников к копировальной и множительной технике |

*Таблица вероятности реализации данной угрозы через уязвимость в течении года(P(V) и критичности реализации угрозы (ER).*

|  |  |  |
| --- | --- | --- |
| *Угроза/уязвимость* | *P(V), %* | *ER,%* |
| 1/1 | 70 | 80 |
| 1/2 | 40 | 60 |
| 2/1 | 30 | 30 |
| 2/2 | 70 | 50 |
| 3/1 | 70 | 50 |
| 3/2 | 90 | 80 |

*Таблица уровня угрозы по определённой уязвимости (Th) и по уровню угроз по всем уязвимостям (CTh).*

|  |  |  |
| --- | --- | --- |
| *Угроза/уязвимость* | *Th* | *CTh* |
| 1/1 | 0,56 | 0,666 |
| 1/2 | 0,24 |
| 2/1 | 0,09 | 0,408 |
| 2/2 | 0,35 |
| 3/1 | 0,35 | 0,818 |
| 3/2 | 0,72 |

Th=P(V)/100\*ER/100

CTh=1-П(1-Th)

Рассчитаем общий уровень угроз по ресурсу:

CThR=1-П(1-CTh)=1-0,334\*0,592\*0,182=0,964

Рассчитаем риск по ресурсу:

R=CTh\*D=0,964\*3000=**2892 (руб).**

Администрация города Миасса является государственной организацией, поэтому деньги на создание комплексной системы защиты информации будут выделяться из городского бюджета.

Из оценки рисков можно подсчитать какой ущерб может понести Администрация при реализации той. Так же мы можем оценить экономическую целесообразность построения КСЗИ.

Если потери при реализации информационных угроз являются незначительными, то не имеет смысла строить дорогостоящую КСЗИ.

Еще одним важным шагом является разработка Технического задания на КСЗИ (Приложение №3).Оно определяет все основные требования к КСЗИ и возможные пути реализации её составляющих элементов. В ТЗ формулируются и исследуются основные каналы утечки информации и пути и средства их локализации.

**Разработка политики безопасности. (Приложение №4)**

Под политикой информационной безопасности (ИБ) понимается совокупность документированных управленческих решений, направленных на защиту информационных ресурсов организации. Это позволяет обеспечить эффективное управление и поддержку политики в области информационной безопасности со стороны руководства организации.

Политика ИБ  является объектом стандартизации. Некоторые  страны имеют национальные стандарты, определяющие основное содержание подобных документов. Имеются ряд ведомственных стандартов и международные стандарты в этой области (ISO 17799).

В России к нормативным документам, определяющим содержание политики ИБ, относится ряд РД ФСТЭКа. В отечественных и международные стандартах   используются  сходная методология, однако ряд вопросов в отечественных РД не рассмотрен или рассмотрен менее подробно.  Таким образом, при разработке политики ИБ целесообразно использовать передовые зарубежные стандарты, позволяющие разработать более качественные документы, полностью соответствующие отечественным РД.

Целью разработки политики организации в области информационной безопасности является определение правильного (с точки зрения организации) способа использования информационных ресурсов, а также разработка процедур, предотвращающих или реагирующих на нарушения режима безопасности.

**Основные этапы:**

Разработка концепции политики информационной безопасности

Описание границ системы и построение модели ИС с позиции безопасности

Анализ рисков: формализация системы приоритетов организации в области информационной безопасности, выявление существующих рисков и оценка их параметров

Анализ возможных вариантов контрмер и оценка их эффективности.

Выбор комплексной системы защиты на всех этапах жизненного цикла

**Заключение.**

Таким образом, поставив перед собой цель разработать проект КСЗИ в Администрации города Миасса, мною были проделаны следующие работы:

1. Я рассмотрела общую характеристику объекта защиты;
2. Построила модель бизнес-процессов с целью выявления конфиденциальной информации;
3. Составила «Перечень сведений конфиденциального характера»;
4. Выявила угрозы, уязвимости и произвела расчет рисков для ключевых объектов защиты;
5. Описала техническое задание
6. Рассмотрела политику безопасности.
7. Получить теоретические знания и практические навыки в создание эффективной системы защиты информации.

Я считаю, что построение КСЗИ в таком муниципальном органе, как городская Администрация необходима.

**Источники**:

1. Грибунин В.Г. Политика безопасности: разработка и реазизация// «Информационная безопасность», 2005, №1.
2. Демин В., Свалов В. Правовое обеспечение системы защиты информации на предприятии.
3. Домарев В.В. Безопасность информационных технологий. Системный подход. - К.: ООО ТИД «Диасофт», 2004. - 992 с.
4. Торокин А.А. «Основы инженерно-технической защиты информации». – М.:
5. Шиверский А.А Защита информации: проблемы теории и практика. М.: Юрист, 1996.
6. Ярочкин В.И. Информационная безопасность: Учебник для студентов Вузов. М.: Академический Проект; Фонд "Мир", 2003, 640 стр

Приложение №3

**«Техническое задание на систему защиты информации»**

|  |
| --- |
| приложение 1  к Договору №\_\_\_\_\_\_\_\_\_\_\_\_от «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_2005г. |

Для служебного пользования

Экз. №\_\_

|  |  |
| --- | --- |
| От Заказчика: | От Исполнителя: |
| Первый заместитель главы города | Генеральный директор ОАО «Безопасность» |
| \_\_\_\_\_\_\_\_\_\_\_ А.С. Бородин | \_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.П. Заикин |
| «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_ 2008 г. | «\_\_\_» \_\_\_\_\_\_\_\_\_\_ 2008 г. |

**Техническое задание**

**на создание КСЗИ Администрации города Миасса.**

**Термины и определения**

ДЛЯ СЛУЖЕБНОГО ПОЛЬЗОВАНИЯ (ДСП) – конфиденциальная информация, которая: либо получена в процессе производственной деятельности от государственных предприятий и организаций, либо создана для государственных организаций при обработке информации, полученной от любых контрагентов. Либо изначальным, либо конечным собственником данной информации ограниченного распространения является государство. От утечки данной информации могут пострадать интересы государства.

ПЕРСОНАЛЬНЫЕ ДАННЫЕ (ПД) - конфиденциальная информация о частной жизни физического лица, которая получена в процессе производственной деятельности от любых контрагентов. Собственником данной информации ограниченного распространения является физическое лицо. От утечки данной информации могут пострадать интересы этого физического лица.

НЕ СЕКРЕТНО (НС) – открытая информация, доступ к которой не ограничивается требованиями безопасности либо согласно производственной необходимости (общий доступ и т.п.), либо как не подлежащая засекречиванию в соответствии с законодательством (данные бухгалтерского учета и т.п.)

КОНТРОЛИРУЕМАЯ ЗОНА (КЗ) - это пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств. Границей КЗ Организации является: периметр охраняемой территории Организации; ограждающие конструкции охраняемого здания или охраняемой части здания.

ОСНОВНЫЕ ТЕХНИЧЕСКИЕ СРЕДСТВА (ОТСС) - технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации. К ним относятся средства вычислительной техники, средства и системы передачи данных, отображения и размножения документов.

ВСПОМОГАТЕЛЬНЫЕ ТЕХНИЧЕСКИЕ СРЕДСТВА (ВТСС) - технические средства и системы, не предназначенные для передачи, обработки и хранения конфиденциальной информации, устанавливаемые совместно с ОТСС. К ним относятся: радио- и телефонные средства и системы; средства и системы охранной и пожарной сигнализации; контрольно-измерительная аппаратура; средства и системы кондиционирования; средства и системы проводной радиотрансляционной и телевизионной сети; средства электронной оргтехники; средства вычислительной техники, не предназначенные для передачи, обработки и хранения конфиденциальной информации.

НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП (НСД) – нарушение установленных правил доступа (организационных, технических и программных ограничений) к конфиденциальной информации, преднамеренное либо не преднамеренное, независимо от результата (получен фактический доступ к этой информации или нет).

ПОБОЧНЫЕ ЭЛЕКТРОМАГНИТНЫЕ ИЗЛУЧЕНИЯ И НАВОДКИ (ПЭМИН) – распространение электромагнитного излучения, возникающего в результате обработки конфиденциальной информации, в окружающем пространстве (по эфиру), а также по металлическим проводникам (коммуникациям), и позволяющего интерпретировать данную информацию.

КОНФИДЕНЦИАЛЬНАЯ ЛОКАЛЬНАЯ ВЫЧИСЛИТЕЛЬНАЯ СЕТЬ (ЛВС) – комплекс средств вычислительной техники, соединенных каналами передачи данных, не выходящими за пределы КЗ, и предназначенных для обработки конфиденциальной информации. ЛВС функционально может являться частью вычислительной сети Организации (в остальных частях обрабатывается не конфиденциальная информация), а организационно – это часть АС, расположенная в пределах КЗ.

**Общая характеристика объекта.**

Предметом защиты является конфиденциальная информация в Администрации города Миасса. Эта информация циркулирует в определенных подразделениях, а также в электронном виде располагается на сервере корпоративной сети.

В этом органе государственно управления конфиденциальная информация создается, обрабатывается, используется и уничтожается.

Выделяют сведения конфиденциального характера на основании следующих документов:

Сведениям различной степени конфиденциальности в соответствии с СТР-К собственниками информации должны присваиваться соответствующие грифы конфиденциальности. На основании анализа входящих документов выявлено следующее:

Конфиденциальная информация в подразделениях Администрации обрабатывается с помощью офисных приложений, ведомственного прикладного программного обеспечения (ПО) с использованием систем управления базами данных (СУБД) и служебных утилит.

Границей КЗ Администрации является ограждающая конструкция территории. Особенностью КЗ является присутствие на контролируемой территории посторонних лиц (ведется прием посетителей).

Телефонная связь в Администрации осуществляется через общую АТС и внутреннюю. Кабели общей АТС выходят за пределы КЗ.

Пожарная и охранная сигнализации установлены во всех помещениях здания.

Электропитание всего здания осуществляется от трансформаторной подстанции, которая расположена на контролируемой территории и обслуживается персоналом станции.

**Доступ к информации.**

Доступ на территорию Администрации осуществляется свободно, кроме второго этаже где находится КПП. Пропускной режим обеспечивается круглосуточно силами сотрудников вневедомственной охраны УВД. Доступ на территорию Администрации и в помещения, где хранится кон информация, осуществляется по служебному удостоверению либо по специальной отметке в пропуске.

Допуск служащих Администрации к защищаемым информационным ресурсам осуществляется в соответствии с должностными обязанностями, утвержденными службой безопасности, и разграничивается штатными средствами ОС. Физический доступ к серверу и активному сетевому оборудованию ограничен, они размещены на втором этаже здания, в отдельном кабинете, в закрывающихся телекоммуникационных шкафах.

Для передачи данных между пользователями АРМ используются автоматизированные системы документооборота (внутренняя электронная почта, средства передачи сообщений).

**Информационная характеристика.**

В технологическом процессе обработки конфиденциальной информации определены следующие компоненты:

* субъекты доступа;
* объекты доступа.

К субъектам доступа относятся:

* служащие, имеющие отношение к процессу функционирования Администрации и которые имеют возможность доступа к её ресурсам;
* процедуры (процессы) обработки данных прикладного и системного ПО, а также СУБД, которые получают данные из файлов и баз данных на сервере.

К объектам доступа относятся:

* информационные ресурсы – отдельные файлы и массивы файлов, поля, записи и таблицы БД, документы, машинные носители информации (НЖМД, НГМД, CD-RW (CD-R) диски), доступ к которым должен регламентироваться правилами разграничения доступа;
* элементы системы – средства обработки и передачи информации (технические и программные средства, средства приема, отображения, перемещения информации, машинные накопители и носители на бумажной основе), доступ к которым необходимо регламентировать.

На ПЭВМ пользователей и на сервере установлены операционные системы семейства Microsoft Windows (XP), но система управления пользователями и разграничения доступа к файловым ресурсам не является централизованной (доменная структура отсутствует).

**Каналы утечки информации.**

К возможным каналам утечки или нарушения целостности информации можно отнести:

* НСД к информации, обрабатываемой на ПЭВМ и на сервере;
* НСД к бумажным и машинным носителям информации;
* выход из строя технических и программных средств, в т.ч. машинных носителей информации.

Нарушение целостности информации возможно как путем физического разрушения носителей информации, так и путем искажения ее с помощью программных средств:

* Аварии, стихийные бедствия (пожар, затопление);
* Колебания в сети электропитания;
* Старение магнитной поверхности носителей информации;
* Ошибочное удаление информации пользователем;
* Сбои прикладного программного обеспечения.

Возможны следующие способы несанкционированного доступа к защищаемым ресурсам АС:

* физический доступ к носителям информации (к серверу) и их резервным копиям с целью их хищения;
* физический доступ к бумажным носителям информации, с целью их хищения, размножения, фотографирования;
* непосредственный (вне рамок прикладного ПО) доступ к файлам хранилища информации, таблицам БД и исполняемым модулям ПО - удаленно или локально с целью их копирования и дальнейшей установки, а также с целью их уничтожения;
* применение нештатных специальных программ, обеспечивающих восстановление удаленных данных с машинных носителей информации;
* передача файлов по каналам связи между сотрудниками и за пределы станции с целью предоставления НСД лицам, не имеющим допуска к данной информации в обход штатных средств защиты;
* доступ в рамках прикладного ПО локально или удаленно к базам данных и файлам с использованием недокументированных возможностей и режимов работы этого ПО, разработанных и установленных в качестве модификаций, в случае, когда разработчиком ПО является сторонняя организация;
* любой доступ к ПО и данным с использованием технологий взлома средств защиты с целью получения или уничтожения данных (в т.ч. компьютерные вирусы);
* доступ с использованием чужого идентификатора, а также с чужого рабочего места во время отсутствия пользователя этого АРМ.

**Модель нарушителя**

В качестве возможного нарушителя рассматривается субъект, имеющий доступ к работе с программными и техническими средствами. Нарушители классифицируются по уровню возможностей, предоставляемых им всеми доступными средствами (Таблица 1).

Таблица 1.

|  |  |  |  |
| --- | --- | --- | --- |
| Уро-вень | Возможности нарушителя по технологическому процессу | Потенциальная группа нарушителей | Возможный результат НСД |
| 1 | Нет | Служащие, не имеющие доступа к информации, но имеющие доступ в помещения (обслуживающий персонал, посетители) | Просмотр на экране монитора и хищение бумажных и машинных носителей. |
| 2 | Запуск задач (программ) из фикси­ро­ванного набора, реализующих заранее предусмотренные функции по обра­ботке информации | Большинство пользователей АС, имеющих непосредственный доступ в помещения, к АРМ, с полномо­чиями, ограниченными на уровне системы защиты информации (СЗИ) | Доступ пользователя к информации другого пользователя в его отсутствие, в т.ч. через сеть, просмотр информации на мониторе (несоблюдение организационных требований). Просмотр и хищение бумажных носителей. |
| 3 | Управление функционированием АС, т.е. воздействие на базовое программное обеспечение ОС и СУБД, на состав и конфигурацию оборудования АС, на настройки СЗИ. Работа с внешними носителями. | Администраторы АС, наделенные неограниченными полномочиями по управлению ресурсами | Доступ администратора АС к информации других пользователей и к средствам СЗИ, непреднамеренное разрушение информации (несоблюдение организационных требований) |
| 4 | Весь объем возможностей лиц, осуществляющих ремонт технических средств АС. | Обслуживающий персонал АС. Специалисты сторонних организаций, осуществляющих поставку и монтаж оборудования для АС | Доступ обслуживающего персонала АС к МН с информацией других пользователей, разрушение информации, установка закладных устройств (несоблюдение организационных требований при ремонте ОТСС) |

**Фактическая защищенность**

Доступ служащих к ресурсам разграничивается штатными средствами ОС. Список служащих, имеющих доступ к ресурсам, документально определен. Доступ ограничивается в соответствии с должностными инструкциями.

Документ, определяющий порядок конфиденциального документооборота существует и утвержден.

Документально определена технология обработки информации (документ «Описание технологического процесса обработки информации»).

На серверах и рабочих станциях применяются операционные системы MS Windows, что позволяет применить сертифицированные средства защиты от НСД. Но также осуществляется обработка информации в СУБД, что практически исключает применение на данных объектах сертифицированных средств защиты от НСД по причине отсутствия таких средств на рынке.

**Перечень мер по защите**

Разработка перечня защищаемой информации

* Необходимо переработать перечень сведений конфиденциального характера в плане детализации обрабатываемых данных и отнесении сведений к той или иной степени конфиденциальности.

Конфиденциальность информации

С целью повышения степени защищенности информации в плане соблюдения конфиденциальности необходимо:

* разделить ввод и вывод информации одного грифа на уровне АРМ или пользователей с целью разделения ответственности и усиления контроля за этими этапами технологического процесса;
* ограничить (в т.ч. организационно) возможности несанкционированного вывода информации пользователями на внешние носители (дискеты, лазерные накопители CD-RW, USB-Flash) и на печать;
* ограничить количество или исключить использование локальных принтеров на АРМ пользователей, назначить ответственных за печать документов на сетевых принтерах;
* исключить доступ пользователей к ресурсам АРМ других пользователей, как на запись, так и на чтение, т.е. возможность создания пользователями общих сетевых ресурсов на своих АРМ. Обмен информацией между пользователями осуществлять через общие ресурсы на серверах;
* если один служащий относится к нескольким категориям пользователей, то при совмещении обязанностей он должен пользоваться разными идентификаторами. Например, администратор может выполнять работу пользователя, но не имеет права делать это с идентификатором администратора.

Целостность информации

С целью повышения степени защищенности информации в плане соблюдения целостности необходимо:

* внедрение исправлений и добавлений централизованно распространяемых ведомственных программных средств на АРМ пользователей и на сервер должно осуществляться в виде уже откомпилированных исполняемых модулей и процедур, в состав которых не должны включаться средства отладки.

**Состав рабочей документации**

Для документального определения режимов обработки и защиты информации в состав рабочей (исполнительной) документации по защите конфиденциальной информации необходимо включить следующие документы:

* «Описание технологического процесса обработки конфиденциальной информации», в котором отражен порядок проведения всех операций ТП (ввод, вывод, обработка и хранение, резервирование и восстановление, управление доступом);
* «Инструкция пользователя», в которой отражены порядок его работы с информацией, права, обязанности и ответственность;
* «Инструкции администраторов ОС, БД»;
* «Инструкция обслуживающего персонала»;
* «Журнал регистрации бумажных носителей информации», в котором учитываются все операции распечатывания документов, графы журнала заполняются исполнителями работ;
* «Журнал учета резервного копирования», в котором учитываются все операции резервного копирования и восстановления информации, все графы журнала заполняют администраторы.
* Перечень сведение конфиденциального характера Администрации города Миасса.

Приложение №4

«Политика безопасности Администрация города Миасса

**УТВЕРЖДАЮ**

Первый заместитель главы города

А.С..Бородин

|  |
| --- |
| Администрация города Миасса |

**Политика**

19.10.2007 г. № 1\_\_

г. Челябинск

**безопасности Администрации города Миасса**

# Общие положения.

# Назначение документа.

Политика является основой для:

1. Разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения безопасности информации;
2. Принятия управленческих решений и разработки практических мер по воплощению политики безопасности информации и выработки комплекса согласованных мер нормативно-правового, технологического и организационно-технического характера, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз безопасности информации;
3. Координации деятельности структурных подразделений Администрации при проведении работ по созданию, развитию и эксплуатации АС с соблюдением требований обеспечения безопасности информации.

## Основания для разработки документа.

1. Приказ главы Администрации города Миасса о создании Политики Информационной Безопасности Администрации.
2. Законодательной базой ПИБ являются: Конституция РФ, Гражданский и Уголовный кодексы, нормативные документы действующего законодательства, документы Федеральной службы технического и экспертного контроля, организационно- распорядительные документы Администрации.

## Основные определения и сокращения.

Информация— сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления

Разглашение КИ – несанкционированный выход защищаемых сведений и документов за пределы круга лиц, которым они доверены или стали известны в ходе их трудовой деятельности.

Разрешительная (разграничительная) система доступа к информации – совокупность обязательных норм, устанавливаемых первым руководителем или коллективным органом руководства фирмой с целью закрепления за руководителями и сотрудниками права использования для выполнения служебных обязанностей выделенных помещений, рабочих мест, определенного состава документов и ценных сведений.

Сервер – аппаратно-программный комплекс, исполняющий функции хранения и обработки запросов пользователей и не предназначенный для локального доступа пользователей ввиду высоких требований по обеспечению надёжности, степени готовности и мер безопасности ИС предприятия.

Автоматизированная станция - совокупность программных и аппаратных средств, предназначенных для хранения, передачи и обработки данных и информации и производства вычислений.

Коммерческая тайна – это конфиденциальная информация, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности её третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны (то есть, приняты меры по охране её конфиденциальности).

Информация о гражданах (персональные данные) — сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность.

Нарушитель – это лицо, которое предприняло попытку выполнения запрещённых операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, с целью самоутверждения и т.п.) и использующее для этого различные методы, возможности и средства.

АРМ – автоматизированное рабочее место

АС – автоматизированная станция

ЗИ – защита информации

ИБ – информационная безопасность

ИТ – информационные технологии

КД – конфиденциальные документы

КИ – конфиденциальная информация

КТ – коммерческая тайна

ЛВС – локальная вычислительная сеть

НДВ – не декларированные возможности

НСД – несанкционированный доступ

ПБ – политика безопасности

ПИ – персональный идентификатор

ПК – персональный компьютер

ПО – программное обеспечение

ПЭВМ – персональная электронно-вычислительная машина

ПЭМИН – побочные электромагнитные излучения и наводки

ОС – операционная система

ЧС – чрезвычайная ситуация

ЭЛТ – электронно-лучевая трубка

# Описание информационной системы.

## Ответственность подразделений.

Ответственность подразделений распределяется следующим образом:

* За поддержание ИС в рабочем состоянии и обеспечение её функционирования ответственно Системный администратор;
* За физическую сохранность оборудование и носителей информации ответственна Служба безопасности;
* За информационную безопасность и обеспечение конфиденциальности информации ответственен специалист по защите информации.

## Режим функционирования системы.

Режим функционирования информационной системы – только в рабочее время. В целях выполнения регламентных работ по обслуживанию оборудования или программного обеспечения системы возможна остановка в работе отдельных элементов системы (сервера.) без ущерба для общей функциональности.

При возникновении сбоев соответствующее сообщение сохраняется подсистемой журнал копирования в системном журнале.

## Цели и задачи политики безопасности.

Цель: обеспечение защиты информации от ее искажения, модификации, утраты, которые могут привести к нарушению работы администрации, как муниципального органа управления.

Задачи политики безопасности:

* выявление действующих и потенциальных угроз;
* разработка методов противодействия выявленным угрозам;

определение оптимального количества сил и средств, необходимых для обеспечения безопасности.

# Средства управления.

## Оценка рисков и управление ими.

## Экспертиза системы ЗИ (существующие средства ЗИ).

## Правила поведения, должностные обязанности и ответственность.

## Планирование безопасности.

## Разрешение на ввод компонентов в строй (любого компонента ИС и системы ЗИ).

## Порядок подключения подсетей подразделений к сетям общего пользования.

# Функциональные средства.

## Защита персонала.

## Управление работой и вводом/выводом информации.

## Планирование непрерывной работы.

## Средства поддержки программных приложений.

Для поддержки программных приложений, системный администратор обязательном порядке, каждое утро проверяет наличие обновлений на сайтах производителей установленного ПО и, при наличии, принимает меры по исправлению сложившейся ситуации.

## Средства обеспечения целостности информации.

В случае обнаружения несовпадения контрольных сумм – осуществляется восстановление данных из резервных копий.

Резервные копии информации и программного обеспечения должны извлекаться и тестироваться на регулярной основе.

## Документирование (вся структура документов по ИС и СЗИ + правила составления документов).

Документация должна включать записи решений руководства для обеспечения отслеживаемости действий к решениям руководства и политикам, а также воспроизводимости записанных результатов.

В структуру документации по системе защиты информации входят:

* Перечень сведений конфиденциального характера;
* Перечень персональных данных;
* Положение о конфиденциальном документообороте;
* Техническое задание на проведение работ по созданию комплексной системы защиты информации;
* Технологический процесс обработки информации в информационной системе;
* Технический паспорт информационной системы;
* Перечень угроз информационной системы;
* Печень объектов защиты.

Разрабатываемая документация оформляется в соответствии с ГОСТ РД 50-34.698-90 и ГОСТ 6.10-84, а так же «Положением о конфиденциальном документообороте».

## Осведомлённость и обучение специалистов.

В целях оперативного оповещения о произошедших инцидентах, плановых и внеплановых работ, ограничении функциональности и изменениях в документах, посвященных системе защиты информации оповещаются все служащие посредствам совещаний..

Все служащие Администрации должны в обязательном порядке проходить обучение по вопросам информационной безопасности. Для персонала непосредственно участвующего в процессе разработки или поддержки функционирования информационной системы и системы безопасности такое обучение должно проходить не реже 1 раза в год, для всего остального персонала – не реже 1 раза в 3 года, для вновь принятых на работу – перед вступлением в должность.

## Ответные действия, в случае возникновения происшествий.

Все инциденты информационной безопасности должны записываться в базу знаний для дальнейшего анализа и выработки решений для предотвращения подобных происшествий в будущем.

Кроме того должны быть разработаны и утверждены инструкции по действиям в аварийных ситуациях (пожар, затопление и др.).

# Технические средства.

## Требования к процедурам идентификации и аутентификации.

Процедуры идентификации и аутентификации должны обеспечивать надёжный контроль доступа к ресурсам ИС.

## Требования к системам контроля разграничения доступа.

Система контроля доступа должна обеспечивать надёжный контроль доступа к ресурсам ИС.

## Требования к системе регистрации событий в ИС.

Система регистрации должна обеспечивать запись всех событий, происходящих в ИС, а так же предоставлять данные записи в удобочитаемом виде, для последующего ознакомления с ними соответствующими сотрудниками.

# ПРИЛОЖЕНИЕ №5

**«Список объектов защиты»**

**УТВЕРЖДАЮ**

Первый заместитель главы города

А.С. Бородин

|  |
| --- |
| Администрация города Миасса |

**СПИСОК**

19.10.2007 г. № 1\_\_

г. Челябинск

**объектов защиты**

1. **Автоматизированные системы различного уровня и назначения**
   1. Автоматизированные рабочие места служащих
   2. АРМ секретаря главы города
   3. АРМ главы города
2. **Системы связи, системы отображения и размножения**
   1. средства и системы телефонной, внутренней телефонной, громкоговорящей связи;
   2. телефонная система «Внутрянняя»
   3. средства и системы звукоусиления;
   4. система конфиденциального делопроизводства (учет, размножение и движение бумажных и прочих внешних носителей информации);
   5. система обработки информации в вычислительной сети (ввод, вычисления, хранение, вывод);
   6. система обработки речевой информации в специально предназначенных (защищаемых) помещениях (переговоры, совещания);
   7. автоматизированная система передачи информации между сетями по неконтролируемой территории (файлы, базы данных, факсы, телефонные разговоры).
3. **Помещения, в которых установлены 1, 2, 3.**
   1. Кабинет главы города
   2. Кабинет секретаря главы города
   3. Архив/серверная
   4. Бухгалтерия
   5. Юридический отдел
   6. Отдел муниципальной службы кадров
   7. Отдел службы безопасности
   8. Отдел по работе с кадрами и защите прав потребителей.

Начальник службы

конфиденциального делопроизводства Н.Н.Ушко

СОГЛАСОВАНО

Начальник службы безопасности Ю.К.Крысова

Начальни службы конфиденциального документооборота Д.Б.Ненашев

Первый заместитель главы города А.С.Бородин

В дело №\_\_\_\_\_\_

# ПРИЛОЖЕНИЕ №6

