# Введение

На современном этапе развития нашего общества многие традиционные ресурсы человеческого прогресса постепенно утрачивают свое первоначальное значение. На смену им приходит новый ресурс, единственный продукт не убывающий, а растущий со временем, называемый информацией. Информация становится сегодня главным ресурсом научно-технического и социально-экономического развития мирового сообщества. Чем больше и быстрее внедряется качественной информации в народное хозяйство и специальные приложения, тем выше жизненный уровень народа, экономический, оборонный и политический потенциал страны.

В настоящее время хорошо налаженная распределенная сеть информационно-вычислительных комплексов способна сыграть такую же роль в общественной жизни, какую в свое время сыграли электрификация, телефонизация, радио и телевидение вместе взятые. Ярким примером этому стало развитие глобальной сети Internet. Уже принято говорить о новом витке в развитии общественной формации - информационном обществе.

Любая предпринимательская деятельность тесно связана с получением, накоплением, хранением, обработкой и использованием разнообразных информационных потоков. Целостность современного мира как сообщества обеспечивается, в основном, за счет интенсивного информационного обмена. Приостановка глобальных информационных потоков даже на короткое время способно привести к не меньшему кризису, чем разрыв межгосударственных экономических отношений. Поэтому в новых рыночно-конкурентных условиях возникает масса проблем, связанных не только с обеспечением сохранности коммерческой (предпринимательской) информации как вида интеллектуальной собственности, но и физических и юридических лиц, их имущественной собственности и личной безопасности.

Учитывая известный афоризм «цель оправдывает средства», информация представляет определенную цену. И поэтому сам факт получения информации злоумышленником приносит ему определенный доход, ослабляя тем самым возможности конкурента. Отсюда главная цель злоумышленника - получение информации о составе, состоянии и деятельности объекта конфиденциальных интересов (фирмы, изделия, проекта, рецепта, технологии и т. д.) в целях удовлетворения своих информационных потребностей. Возможно в корыстных целях и внесение определенных изменений в состав информации, циркулирующей на объекте конфиденциальных интересов. Такое действие может привести к дезинформации по определенным сферам деятельности, учетным данным, результатам решения некоторых задач. Более опасной целью является уничтожение накопленных информационных массивов в документальной или магнитной форме и программных продуктов. В связи с этим все большее значение приобретает организация эффективной системы информационной безопасности.

**Информационной безопасностью называют меры по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе. Информационная безопасность включает в себя меры по защите процессов создания данных, их ввода, обработки и вывода. Целью информационной безопасности является обезопасить ценности системы, защитить и гарантировать точность и целостность информации, и минимизировать разрушения, которые могут иметь место, если информация будет модифицирована или разрушена. Информационная безопасность требует учета всех событий, в ходе которых информация создается, модифицируется, к ней обеспечивается доступ или она распространяется.**

Целью данной курсовой работы является обеспечение защиты данных в информационной системе предприятия ООО магазин «Стиль».

Исходя из поставленной цели, необходимо решить следующие задачи:

1. Обследовать существующую инфраструктуру ООО магазин «Стиль» и определить исходные данные для проектирования системы ИБ;
2. Определить минимальные требования на основе потребностей в ИБ;
3. Разработать концепцию ИБ;
4. Проанализировать риски;
5. Разработать политику ИБ и выбрать решения по обеспечении политики ИБ;
6. Разработать систему информационной безопасности.

# 1. Обследование существующей инфраструктуры и определение исходных данных для проектирования системы ИБ

# 1.1 Организационная структура

Полное фирменное наименование: Общество с ограниченной ответственностью магазин «Стиль».

Сокращенное наименование: ООО магазин «Стиль».

Орган, осуществивший государственную регистрацию: Росстат Территориальный орган Федеральной службы Государственной статистики по Омской области (ОмскСтат).

Дата государственной регистрации компании: 03.03.1999 г. Номер свидетельства о государственной регистрации: ОГРН – 1046182528418.

Адрес места нахождения: 644010, Россия, Омская область, г. Омск, ул. Ленинградская площадь 1.

Юридический адрес: 644010, Россия, Омская область, г. Омск, ул. Ленинградская площадь 1.

Почтовый адрес: 644010, Россия, Омская область, г. Омск, ул. Ленинградская площадь 1.

Тел.: (3812) 58–07–79;

Руководство: Генеральный директор – Узкова Лариса Александровна.

ООО магазин «Стиль» осуществляет розничную продажу одежды и обуви. Основной целью организации, как полностью коммерческого предприятия, состоит в получении прибыли от своей деятельности и максимально длительный срок оставаться на рынке, стремясь расширять свой ассортимент и рынок сбыта.

Предприятие работает с множеством различных поставщиков. Заказ товара происходит по телефону. Оплата товара поставщикам осуществляется путем безналичного расчета платежным поручением.

Процесс продаж происходит следующим образом: клиент покупает необходимые комплектующие в розницу через розничный магазин предприятия. Расчет производится наличными деньгами через кассу. Все обслуживание клиентов осуществляется продавцами розничного магазина.

Бухгалтерскую документацию ведут бухгалтера. Они также занимаются сдачей регулярных отчетов в налоговую службу.

# 1.2 Состав и выполняемые функции должностных лиц

Персонал предприятия:

* директор – осуществляет непосредственное руководство процессами организации, производит безналичные расчеты с поставщиками и покупателями, производит анализ прошлых продаж и принимает заявки от менеджера на заказ товаров, на основе анализа и заявок производит заказ необходимых товаров у поставщиков, ищет возможности для расширения ассортимента;
* менеджер – передаёт директору заявки на заказ товаров у поставщиков;
* продавцы – производят розничную реализацию в торговом зале, после продажи товаров делают отметки в базе данных о количестве реализованной продукции, являются ответственным за хранение комплектующих;
* системный администратор – осуществляет настройку и установку оборудования, занимается устранением неполадок с ПО и компьютерным оборудованием, следит за работоспособностью компьютеров и периферийного оборудования.
* Бухгалтерия ООО магазин «Стиль» осуществляет сплошное, непрерывное, взаимосвязанное, документальное отражение хозяйственной деятельности данного предприятия.

Функции данного отдела организации возлагаются на соответствующие должностные лица (бухгалтеров), которые производят учет, необходимый для характеристики отдельных сторон деятельности компании. Указанные должностные лица несут ответственность за правильное и своевременное оформление хозяйственных операций, а также обеспечивают сохранность и учет денежных средств, циркулирующих в процессе осуществления хозяйственной деятельности организации.

С бухгалтерами заключаются договоры о полной материальной ответственности в соответствии с законодательством РФ.

Организационная структура предприятия в виде графической схемы представлена на рисунке 1.

Рисунок 1. Организационная структура ООО магазин «Стиль»

Директор

Менеджер

Бухгалтерия

Продавцы

Системный администратор

#

# 1.3 Состав и назначение аппаратных и программных средств

ЛВС бухгалтерии ООО магазин «Стиль» создана с учетом единых концептуальных положений, лежащих в основе построения современных вычислительных сетей связи. Основу таких положений в первую очередь составляет использование общих принципов построения и однородного активного сетевого оборудования.

Сетевая структура ЛВС компании содержит несколько выраженных иерархических уровней. ЛВС бухгалтерии представляет фрагмент корпоративной сети, данный фрагмент сети состоит из нескольких сегментов, подключенных к магистрали более высокого уровня и осуществляющих доступ информационным ресурсам сети. ЛВС построена на базе стандарта Ethernet 10/100 Base-T.

Стандарт Ethernet 10/100 Base-T подходит для работы с различными операционными системами и сетевым оборудованием. Применение этого стандарта позволяет простыми методами добиться стабильной работы сети.

Для построения сети необходимо выбрать кабель, от качества и характеристик которого во многом зависит качество работы сети. В данном случае использована неэкранированная витая пара категории 5.

Конфигурация сети представлена в таблице 1.

Таблица 1

|  |  |
| --- | --- |
| Компонент/характеристика | Реализация |
| Топология | Звезда |
| Линия связи | Неэкранированная витая пара категории 5 |
| Сетевые адаптеры | Ethernet 10/100 Base-T |
| Коммуникационное оборудование | Коммутатор Ethernet 10/100 Base-T |
| Совместное использование периферийных устройств | Подключение сетевых принтеров через компьютеры к сетевому кабелю. Управление очередями к принтерам осуществляется с помощью программного обеспечения компьютеров. |
| Поддерживаемые приложения | Организация коллективной работы в среде электронного документооборота, работа с базой данных. |

При выборе сетевых компонентов необходимо придерживаться следующих общих требований:

* компьютеры должны обладать хорошим быстродействием, чтобы обеспечить работу всех сетевых служб и приложений в реальном времени без заметного замедления работы;
* жесткие диски компьютеров должны быть максимально надежными для того, чтобы обеспечить безопасность и целостность хранимых данных;
* сетевые принтеры должны устанавливаться в зависимости от местоположения пользователей, активно их использующих;
* коммутатор, являющийся центральным устройством данной сети, необходимо располагать в легкодоступном месте, чтобы можно было без проблем подключать кабели и следить за индикацией.

Перечисленные требования определили следующую конфигурацию сетевых компонентов: все компьютеры сети на базе процессора Intel Pentium 4, в качестве сетевого принтера выбрано многофункциональное устройство (лазерное), поскольку они имеют наибольший ресурс и малые затраты на расходные материалы.

Конфигурация рабочих станций приведена в таблице 3.

Таблица 3

| Наименование товара | Количество, шт. |
| --- | --- |
| Материнская плата MSI 945G Neo2-F (i945G, LGA775, Dual DDRII-667, Video, LAN, ATX) | 3 |
| Процессор Intel Celeron D 346 (3,06 Ghz, LGA775, EM64T) | 3 |
| Оперативная память Transcend DIMM 512MB DDRII-533 | 3 |
| Жесткий диск Seagate Barracuda 7200.9 ST3120814A 120,0Gb (U-ATA, 7200 rpm) | 3 |
| Корпус InWin S523T (MidiTower, ATX, USB, 350Вт, Fan, белый) | 3 |
| Монитор NEC (LCD) AccuSync 73V (17", 1280x1024, 500:1) | 3 |
| Мышь Genius NetScroll Eye Mouse (оптика, PS/2) | 3 |
| Клавиатура Logitech Value Keyboard (PS/2) | 3 |

Конфигурация сетевого оборудования приведена в таблице 4.

Таблица 4

|  |  |
| --- | --- |
| Наименование товара | Количество |
| Коммутатор D-Link DES-1016D (UTP, 16 x 10/100) | 1 шт. |
| Кабель UTP (Alcatel, категория 5) | 40 м. |
| Коннектор RJ-45 (категория 5) | 6 шт. |

Конфигурация периферийного оборудования приведена в таблице 5.

Таблица 5

| Наименование товара | Количество, шт. |
| --- | --- |
| Принтер Hewlett Packard LaserJet P2015 (A4, 1200dpi, 26 ppm, 32Mb, USB 2.0) | 1 |

Конфигурация программного обеспечения приведена в таблице 6.

Таблица 6

| Наименование товара | Количество, шт. |
| --- | --- |
| Windows Server 2003 Std Russian R2 (OEM) | 1 |
| Windows XP Professional Russian SP2 (OEM) | 3 |
| Office 2003 Standart Edition Russian SP2 (Коробка) | 3 |
| 1С:Бухгалтерия 7.7 | 1 |
| Лицензия на 10 доп. рабочих мест для «1С: Бухгалтерия 7.7» | 1 |
| Лицензия на сервер для «1С: Бухгалтерия 7.7» | 1 |
| Kaspersky Enterprise Space Security | 1 |

Таким образом, с помощью программных и аппаратных средств в бухгалтерии ООО магазин «Стиль» решаются следующие задачи:

1. Организация общедоступной базы данных с помощью бухгалтерской программы «1С: Бухгалтерия 7.7».
2. Совместная обработка информации пользователями.
3. Централизованное резервное копирование всех данных.
4. Контроль за доступом к данным.
5. Совместное использование оборудования и программного обеспечения.

План помещения показан на рис. 2.

Рисунок 2. План помещения ООО магазин «Стиль»

# 1.4 Основные цели защиты информации на предприятии

Формулирование целей и задач защиты информации, как любой другой деятельности, представляет начальный и значимый этап обеспечения безопасности информации. Важность этого этапа часто недооценивается и ограничивается целями и задачами, напоминающими лозунги. В то же время специалисты в области системного анализа считают, что от четкости и конкретности целей и постановок задач во многом зависит успех в их достижении и решении. Провал многих, в принципе полезных, начинаний обусловлен именно неопределенностью и расплывчатостью целей и задач, из которых не ясно, кто, что и за счет какого ресурса предполагает решать продекларированные задачи.

Цели защиты информации сформулированы в ст. 20 Закона РФ «Об информации, информатизации и защите информации»:

* предотвращение утечки, хищения, искажения, подделки информации;
* предотвращение угроз безопасности личности, общества, государства;
* предотвращение несанкционированных действий по уничтожению, модификации, копированию, блокированию информации, предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима как объекта собственности;
* защита конституционных прав граждан по сохранению личной тайны, конфиденциальности персональных данных, имеющихся в информационных системах;
* сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством;
* обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологии и средств их обеспечения.

В общем виде цель защиты информации определяется как обеспечение безопасности информации, содержащей государственную или иные тайны. Но такая постановка цели содержит неопределенные понятия: информация и безопасность.

Основной целью защиты информации является обеспечение заданного уровня ее безопасности. Под заданным уровнем безопасности информации понимается такое состояние защищенности информации от угроз, при которых обеспечивается допустимый риск ее уничтожения, изменения и хищения. При этом под уничтожением информации понимается не только ее физическое уничтожение, но и стойкое блокирование санкционированного доступа к ней. В общем случае при блокировке информации в результате неисправности замка или утери ключа сейфа, забытия пароля компьютера, искажения кода загрузочного сектора винчестера или дискетки и других факторах информация не искажается и не похищается и при определенных усилиях доступ к ней может быть восстановлен. Следовательно, блокирование информации прямой угрозы ее безопасности не создает. Однако при невозможности доступа к ней в нужный момент ее пользователь теряет информацию так же, как если бы она была уничтожена.

# 1.5 Перечень конфиденциальной информации и информации, составляющей коммерческую тайну

Коммерческая тайна − форма обеспечения безопасности наиболее важной коммерческой информации, предлагающая ограничение ее распространения. С правовой точки зрения, коммерческая тайна предприятия представляет собой средство защиты против недобросовестной конкуренции в рамках реализации права на интеллектуальную собственность.

Перечень сведений, составляющих коммерческую тайну предприятия:

* 1. Производство
	2. Сведения о структуре производства, производственных мощностях, типе и размещении оборудования, запасах сырья, материалов, комплектующих и готовой продукции.

2. Управление

2.1. Сведения о применяемых оригинальных методах управления предприятием.

2.2. Сведения о подготовке, принятии и исполнении отдельных решений руководства предприятия по коммерческим, организационным, производственным, научно-техническим и иным вопросам.

3. Планы

3.1. Сведения о планах расширения или свертывания производства различных видов продукции и их технико-экономических обоснованиях. 3.2.Сведения о планах инвестиций, закупок, продаж. 4. Совещания

4.1. Сведения о фактах проведения, целях, предмете и результатах совещаний и заседаний органов управления предприятия. 5. Финансы

5.1. Сведения о балансах предприятия.

5.2. Сведения, содержащиеся в бухгалтерских книгах предприятия. 5.3. Сведения о кругообороте средств предприятия.

5.4. Сведения о финансовых операциях предприятия.

5.5. Сведения о состоянии банковских счетов предприятия и производимых операциях.

5.6. Сведения об уровне доходов предприятия.

5.7. Сведения о долговых обязательствах предприятия.

5.8. Сведения о состоянии кредита предприятия (пассивы и активы). 6. Рынок

6.1. Сведения о применяемых предприятием оригинальных методах изучения рынка.

6.2. Сведения о результатах изучения рынка, содержащие оценку состояния и перспектив развития рыночной конъюнктуры.

6.3. Сведения о рыночной стратегии предприятия.

6.4. Сведения о применяемых предприятием оригинальных методах осуществления продаж.

6.5. Сведения об эффективности коммерческой деятельности предприятия. 7. Партнеры

7.1. Систематизированные сведения о внутренних и зарубежных заказчиках, подрядчиках, поставщиках, потребителях, покупателях, компаньонах, спонсорах, посредниках, клиентах и других партнерах деловых отношений предприятия, а также о его конкурентах, которые не содержатся в открытых источниках (справочниках, каталогах и др.).

8. Переговоры

8.1. Сведения о подготовке и результатах проведения переговоров с деловыми партнерами предприятия.

9. Контракты

9.1. Сведения, условия конфиденциальности которых установлены в договорах, контрактах, соглашениях и других обязательствах предприятия. 10. Цены

10.1. Сведения о методах расчета, структуре, уровне цен на продукцию и размерах скидок.

11. Торги, аукционы

11.1. Сведения о подготовке к торгам или аукциону и их результатах. 12. Наука и техника

12.1. Сведения о целях, задачах, программах перспективных научных исследований.

12.2. Ключевые идеи НИР.

12.3. Точные значения конструкционных характеристик создаваемых изделий и оптимальных параметров разрабатываемых технологических процессов (размеры, объемы, конфигурация, процентное содержание компонентов, температура, давление, время и т.д.).

12.4. Аналитические и графические зависимости, отражающие найденные закономерности и взаимосвязи.

12.5. Данные об условиях экспериментов и оборудования, на котором они проводились.

12.6. Сведения о материалах, из которых изготовлены отдельные детали.

12.7. Сведения об особенностях конструкторско-технологического, художественно-технического решения изделия, дающие положительный экономический эффект.

12.8. Сведения о методах защиты от подделки товарных знаков.

12.9. Сведения о состоянии программного и компьютерного обеспечения. 13. Технология

13.1. Сведения об особенностях используемых и разрабатываемых технологий и специфике их применения.

14. Безопасность

14.1. Сведения о порядке и состоянии организации защиты коммерческой тайны.

14.2. Сведения, составляющие коммерческую тайну предприятий-партнеров и переданные на доверительной основе.

Правильная организация конфиденциального делопроизводства в фирме является составной частью комплексного обеспечения безопасности информации и имеет важное значение в достижении цели ее защиты. Как известно, специалисты, занимающиеся в области информационной безопасности утверждают, что порядка 80% конфиденциальной информации находится в документах делопроизводства. Поэтому вопросы конфиденциального документооборота в фирме несомненно играют важную роль в достижении ею экономических успехов.

А, следовательно, и документы, содержащие ту или иную информацию подразделяются на секретные и конфиденциальные. Причем, секретные документы могут быть с грифом "Секретно", "Совершенно секретно", "Особой важности". Конфиденциальные документы соответственно с грифами "Коммерческая тайна", "Банковская тайна" и т.д. В настоящее время видов конфиденциальной информации (а, следовательно, и возможных грифованных документов) насчитывается более 30. Что в целом не создает благоприятной атмосферы в смысле обеспечения их безопасности. По этой причине количество видов конфиденциальной информации в перспективе надо полагать уменьшится.

ИT-ресурсы ООО магазин «Стиль» делятся на три группы:

1. Информация, являющаяся коммерческой тайной.
2. Конфиденциальная информация.
3. Информация общего доступа.

Сведения, относящиеся к эти трем группам, сроки действия и условия прекращений ограничений на доступ, а также ограничительный гриф приведены в табл. 8.

Таблица 8

Перечень сведений, составляющих коммерческую тайну ООО «Стиль»

|  |  |  |  |
| --- | --- | --- | --- |
| №п/п | Наименование сведений | Срок действия, условия прекращения ограничений на доступ | Ограничительный гриф |
| 1. Сведения делового характера |
| 1.1 | Информация о номерах домашних телефонов и адресах работников и членов их семей. Местонахождение руководителей, учредителей и членов их семей. Конфликтные ситуации и другие внутренние отношения | Постоянно | Коммерческая тайна |
| 1.2 | Учредительные документы ООО «Стиль» | Постоянно | Конфиденциально |
| 1.3 | Информация, раскрывающая детальные планы капитальных вложений в развитие предприятия. Перспективные и текущие планы развития и роста ООО «Стиль» | До реализации планов | Коммерческая тайна |
| 1.5 | Планы и методы продвижения услуг на рынок, планируемые новые рынки и услуги | До момента реализации планов | Коммерческая тайна |
| 1.7 | Информация об участии (подготовке) компании в торгах и аукционах | До момента завершения торгов | Коммерческая тайна |
| 2. Информация по организационно-правовым вопросам |
| 2.1 | Информация по делам, рассматриваемым в судах, разглашение которой может нанести ущерб интересам компании  | До потери актуальности | Коммерческая тайна |
| 2.2 | Информация, на конфиденциальности которой настаивает хотя бы одна из договаривающихся сторон | До принятия согласованного решения об их раскрытии | Коммерческая тайна |
| 3. Информация по вопросам торгово-экономических отношений |
| 3.2 | Номенклатура и количество услуг по взаимным обязательствам | До потери актуальности | Информация общего доступа |
| 4. Информация по финансово-хозяйственным вопросам |
| 4.1 | Сведения об открытых расчетных и иных счетах, в том числе и в иностранной валюте), о движении средств по эти счетам, о имеющихся вкладах. Операции по банковским счетам | Постоянно | Конфиденциально |
| 4.2 | Информация об особых сделках или условиях платежа по бартерным операциям, об условиях компенсационных сделок | 3 года | Конфиденциально |
| 4.3 | Данные о состоянии дебиторской задолженности, а также о заключенных договорах и соглашениях | До принятия решения об их раскрытии | Конфиденциально |
| 4.4 | Акты комплексных проверок финансово-хозяйственной деятельности ООО «Стиль» (кроме заключений ревизионной комиссии и аудитора) | Постоянно | Конфиденциально |
| 4.5 | Информация об условиях проведения зачетов и вексельных операций по дебиторской и кредиторской задолженностям | 3 года | Конфиденциально |
| 4.6 | Информация об эффективности сделок, договоров | 1 год после прекращения действия договора | Информация общего доступа |
| 4.7 | ИНН, документы об уплате налогов и обязательных платежах | Постоянно | Конфиденциально |
| 4.8 | Акты проверки финансово-хозяйственной деятельности региональных филиалов и компании в целом, проведенные специалистами по аудиту | Постоянно | Конфиденциальнона |

|  |
| --- |
| 5. Информация о производственной деятельности |
| 5.1 | Штатное расписание | Постоянно | Информация общего доступа |
| 5.2 | Сведения об обработанных и необработанных заказах | Постоянно | Информация общего доступа |
| 5.3 | Разрабатываемые проекты по автоматизации предприятий и бизнес-процессов | Постоянно | Коммерческая тайна |
| 5.4 | Консалтинговые услуги: постановка управленческого учета на предприятии, внедрение систем бюджетирования  | Постоянно | Коммерческая тайна |
| 6. По вопросам обеспечения безопасности |
| 6.1 | Информация об организации и состоянии физической охраны административного здания ООО «Стиль», пропускном режиме, установленных системах сигнализации и видеонаблюдения | До потери актуальности | Конфиденциально |

|  |  |  |  |
| --- | --- | --- | --- |
| 6.2 | Информация, раскрывающая организацию, средства и методы обеспечения безопасности ООО «Стиль» | Постоянно | Конфиденциально |
| 6.3 | Информация о защищаемых информационных ресурсах | Постоянно | Конфиденциально |
| 6.4 | Базы данных ООО «Стиль» | Постоянно | Конфиденциально |
| 6.5 | Информация о детальной структуре корпоративной сети | Постоянно | Конфиденциально |
| 6.7 | Сведения о системе разграничения доступа к информации, правах пользователей, ограничениях на использование информационных ресурсов | На период действия | Конфиденциально |
| 7. По организационно-управленческой деятельности |
| 7.1 | Условия индивидуальных трудовых договоров с работниками и руководителями ООО «Стиль» | Постоянно | Конфиденциально |

|  |  |  |  |
| --- | --- | --- | --- |
| 7.2 | Информация о персональных данных работников ООО «Стиль», внесенная в личные дела, а также информация об условиях оплаты труда и премирования | Постоянно | Конфиденциально |
| 7.3 | Информация о персональных данных работников ООО «Стиль», индивидуальных размерах оплаты труда, предоставляемые для проведения актуарных расчетов по негосударственному пенсионному обеспечению | Постоянно | Конфиденциально |

#

# 2. Предпроектное обследование информационной безопасности отдела бухгалтерии ООО магазин «Стиль»

#

# 2.1 Информационная безопасность в вычислительной сети

#

# 2.1.1 Классификация угроз безопасности информации

Под угрозой безопасности информации в компьютерной сети (КС) понимают событие или действие, которое может вызвать изменение функционирования КС, связанное с нарушением защищенности обрабатываемой в ней информации.

# Уязвимость информации — это возможность возникновения такого состояния, при котором создаются условия для реализации угроз безопасности информации.

# Атакой на КС называют действие, предпринимаемое нарушителем, которое заключается в поиске и использовании той или иной уязвимости. Иначе говоря, атака на КС является реализацией угрозы безопасности информации в ней.

# Проблемы, возникающие с безопасностью передачи информации при работе в компьютерных сетях, можно разделить на три основных типа:

# перехват информации – целостность информации сохраняется, но её конфиденциальность нарушена;

# модификация информации – исходное сообщение изменяется либо полностью подменяется другим и отсылается адресату;

# подмена авторства информации. Данная проблема может иметь серьёзные последствия. Например, кто-то может послать письмо от чужого имени (этот вид обмана принято называть спуфингом) или Web – сервер может притворяться электронным магазином, принимать заказы, номера кредитных карт, но не высылать никаких товаров.

# Специфика компьютерных сетей, с точки зрения их уязвимости, связана в основном с наличием интенсивного информационного взаимодействия между территориально разнесенными и разнородными (разнотипными) элементами.

# Уязвимыми являются буквально все основные структурно-функциональные элементы КС: рабочие станции, серверы (Host-машины), межсетевые мосты (шлюзы, центры коммутации), каналы связи и т.д.

# Известно большое количество разноплановых угроз безопасности информации различного происхождения. В литературе встречается множество разнообразных классификаций, где в качестве критериев деления используются виды порождаемых опасностей, степень злого умысла, источники появления угроз и т.д. Одна из самых простых классификаций приведена на рис. 3.

Угрозы безопасности

Естественные

Искусственные

Преднамеренные

Непреднамеренные

Рис. 3. Общая классификация угроз безопасности

Естественные угрозы - это угрозы, вызванные воздействиями на КС и ее элементы объективных физических процессов или стихийных природных явлений, независящих от человека.

Искусственные угрозы - это угрозы КС, вызванные деятельностью человека. Среди них, исходя из мотивации действий, можно выделить:

непреднамеренные (неумышленные, случайные) угрозы, вызванные ошибками в проектировании КС и ее элементов, ошибками в программном обеспечении, ошибками в действиях персонала и т.п.;

преднамеренные (умышленные) угрозы, связанные с корыстными устремлениями людей (злоумышленников).

Источники угроз по отношению к КС могут быть внешними или внутренними (компоненты самой КС - ее аппаратура, программы, персонал).

Анализ негативных последствий реализации угроз предполагает обязательную идентификацию возможных источников угроз, уязвимостей, способствующих их проявлению и методов реализации. И тогда цепочка вырастает в схему, представленную на рис. 4.

Рис. 4. Модель реализации угроз информационной безопасности

Угрозы классифицируются по возможности нанесения ущерба субъекту отношений при нарушении целей. Ущерб может быть причинен каким-либо субъектом (преступление, вина или небрежность), а также стать следствием, не зависящим от субъекта проявлений. Угроз не так уж и много. При обеспечении конфиденциальности информации это может быть хищение (копирование) информации и средств ее обработки, а также ее утрата (неумышленная потеря, утечка). При обеспечении целостности информации список угроз таков: модификация (искажение) информации; отрицание подлинности информации; навязывание ложной информации. При обеспечении доступности информации возможно ее блокирование, либо уничтожение самой информации и средств ее обработки.

Все источники угроз можно разделить на классы, обусловленные типом носителя, а классы на группы по местоположению (рис. 5а). Уязвимости также можно разделить на классы по принадлежности к источнику уязвимостей, а классы на группы и подгруппы по проявлениям (рис. 5б). Методы реализации можно разделить на группы по способам реализации (рис. 5в). При этом необходимо учитывать, что само понятие «метод», применимо только при рассмотрении реализации угроз антропогенными источниками. Для техногенных и стихийных источников это понятие трансформируется в понятие «предпосылка».

Рис. 5. Структура классификаций: а) «Источники угроз»; б) «Уязвимости»; в) «Методы реализации»

Классификация возможностей реализации угроз (атак), представляет собой совокупность возможных вариантов действий источника угроз определенными методами реализации с использованием уязвимостей, которые приводят к реализации целей атаки. Цель атаки может не совпадать с целью реализации угроз и может быть направлена на получение промежуточного результата, необходимого для достижения в дальнейшем реализации угрозы. В случае такого несовпадения атака рассматривается как этап подготовки к совершению действий, направленных на реализацию угрозы, т.е. как «подготовка к совершению» противоправного действия. Результатом атаки являются последствия, которые являются реализацией угрозы и/или способствуют такой реализации.

Исходными данными для проведения оценки и анализа угроз безопасности при работе в сети служат результаты анкетирования субъектов отношений, направленные на уяснение направленности их деятельности, предполагаемых приоритетов целей безопасности, задач, решаемых в сети и условий расположения и эксплуатации сети.

2.1.2 Наиболее распространенные угрозы

Самыми частыми и самыми опасными (с точки зрения размера ущерба) являются непреднамеренные ошибки штатных пользователей, операторов, системных администраторов и других лиц, обслуживающих компьютерную сеть.

Иногда такие ошибки и являются собственно угрозами (неправильно введенные данные или ошибка в программе, вызвавшая крах системы), иногда они создают уязвимые места, которыми могут воспользоваться злоумышленники (таковы обычно ошибки администрирования). По некоторым данным, до 65% потерь - следствие непреднамеренных ошибок.

Пожары и наводнения не приносят столько бед, сколько безграмотность и небрежность в работе.

Очевидно, самый радикальный способ борьбы с непреднамеренными ошибками - максимальная автоматизация и строгий контроль.

Другие угрозы доступности можно классифицировать по компонентам КС, на которые нацелены угрозы:

отказ пользователей;

внутренний отказ сети;

отказ поддерживающей инфраструктуры.

Обычно применительно к пользователям рассматриваются следующие угрозы:

нежелание работать с информационной системой (чаще всего проявляется при необходимости осваивать новые возможности и при расхождении между запросами пользователей и фактическими возможностями и техническими характеристиками);

невозможность работать с системой в силу отсутствия соответствующей подготовки (недостаток общей компьютерной грамотности, неумение интерпретировать диагностические сообщения, неумение работать с документацией и т.п.);

невозможность работать с системой в силу отсутствия технической поддержки (неполнота документации, недостаток справочной информации и т.п.).

Основными источниками внутренних отказов являются:

отступление (случайное или умышленное) от установленных правил эксплуатации;

выход системы из штатного режима эксплуатации в силу случайных или преднамеренных действий пользователей или обслуживающего персонала (превышение расчетного числа запросов, чрезмерный объем обрабатываемой информации и т.п.);

ошибки при (пере)конфигурировании системы;

отказы программного и аппаратного обеспечения;

разрушение данных;

разрушение или повреждение аппаратуры.

По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы:

нарушение работы (случайное или умышленное) систем связи, электропитания, водо- и/или теплоснабжения, кондиционирования;

разрушение или повреждение помещений;

невозможность или нежелание обслуживающего персонала и/или пользователей выполнять свои обязанности (гражданские беспорядки, аварии на транспорте, террористический акт или его угроза, забастовка и т.п.).

Весьма опасны так называемые "обиженные" сотрудники - нынешние и бывшие. Как правило, они стремятся нанести вред организации - "обидчику", например:

испортить оборудование;

встроить логическую бомбу, которая со временем разрушит программы и/или данные;

удалить данные.

Обиженные сотрудники, даже бывшие, знакомы с порядками в организации и способны нанести немалый ущерб. Необходимо следить за тем, чтобы при увольнении сотрудника его права доступа (логического и физического) к информационным ресурсам аннулировались.

2.1.3 Вредоносное программное обеспечение

Одним из опаснейших способов проведения атак является внедрение в атакуемые системы вредоносного программного обеспечения.

Выделяют следующие аспекты вредоносного ПО:

вредоносная функция;

способ распространения;

внешнее представление.

Часть, осуществляющая разрушительную функцию, предназначается для:

внедрения другого вредоносного ПО;

получения контроля над атакуемой системой;

агрессивного потребления ресурсов;

изменения или разрушения программ и/или данных.

По механизму распространения различают:

вирусы - код, обладающий способностью к распространению (возможно, с изменениями) путем внедрения в другие программы;

"черви" - код, способный самостоятельно, то есть без внедрения в другие программы, вызывать распространение своих копий по сети и их выполнение (для активизации вируса требуется запуск зараженной программы).

Вирусы обычно распространяются локально, в пределах узла сети; для передачи по сети им требуется внешняя помощь, такая как пересылка зараженного файла. "Черви", напротив, ориентированы в первую очередь на путешествия по сети.

Иногда само распространение вредоносного ПО вызывает агрессивное потребление ресурсов и, следовательно, является вредоносной функцией. Например, "черви" "съедают" полосу пропускания сети и ресурсы почтовых систем.

Вредоносный код, который выглядит как функционально полезная программа, называется троянским. Например, обычная программа, будучи пораженной вирусом, становится троянской; порой троянские программы изготавливают вручную и подсовывают доверчивым пользователям в какой-либо привлекательной упаковке (обычно при посещении файлообменных сетей или игровых и развлекательных сайтов).

# 2.2 Разработка концепции ИБ

# 2.2.1 Цели и задачи информационной безопасности

Режим информационной безопасности – это комплекс организационных и программно-технических мер, которые должны обеспечивать следующие параметры:

* доступность и целостность информации;
* конфиденциальность информации;
* невозможность отказа от совершенных действий;
* аутентичность электронных документов.

Цель информационной безопасности - обеспечить бесперебойную работу организации и свести к минимуму ущерб от событий, таящих угрозу безопасности, посредством их предотвращения и сведения последствий к минимуму.

К задачам информационной безопасности бухгалтерии ООО магазин «Стиль» относится:

* объективная оценка текущего состояния информационной безопасности;
* обеспечение защиты и надежного функционирования прикладных информационных сервисов;
* обеспечение безопасного доступа в Интернет с защитой от вирусных атак и спама;
* защита системы электронного документооборота;
* организация защищенного информационного взаимодействия с территориально удаленными офисами и мобильными пользователями;
* получение защищенного доступа к информационной системе организации;
* обеспечение целостности и доступности информации;
* предотвращение некорректного изменения и модификации данных.

# 2.2.2 Общие направления информационной безопасности

Проблема обеспечения необходимого уровня защиты информации – весьма сложная задача, требующая для своего решения не просто осуществления некоторой совокупности научных, научно-технических и организационных мероприятий и применения специфических средств и методов, а создания целостной системы организационных мероприятий и применения специфических средств и методов по защите информации.

В рамках комплексного подхода к внедрению системы безопасности для бухгалтерии ООО «Стиль» можно выделить следующие общие направления:

* внедрение решений по сетевой безопасности с применением средств компьютерной защиты информации;
* внедрение систем однократной аутентификации (SSO);
* внедрение системы контроля целостности информационной системы;
* внедрение решений по мониторингу и управлению информационной безопасностью;
* внедрение системы контроля доступа к периферийным устройствам и приложениям;
* внедрение систем защиты от модификации и изменения информации.

Основными требованиями к комплексной системе защиты информации являются:

* система защиты информации должна обеспечивать выполнение

информационной системой своих основных функций без существенного ухудшения характеристик последней;

* система защиты должна быть экономически целесообразной;
* защита информации должна обеспечиваться на всех этапах жизненного цикла, при всех технологических режимах обработки информации, в том числе при проведении ремонтных и регламентных работ;
* в систему защиты информации должны быть заложены возможности ее совершенствования и развития в соответствии с условиями эксплуатации и конфигурации;
* система защиты в соответствии с установленными правилами должна обеспечивать разграничение доступа к конфиденциальной информации с отвлечением нарушителя на ложную информацию, т.е. обладать свойствами активной и пассивной защиты;
* система защиты должна позволять проводить учет и расследование случаев нарушения безопасности информации;
* применение системы защиты не должно быть сложной для пользователя, не вызывать психологического противодействия и желания обойтись без нее.

# 2.2.3 Основные аспекты, решаемые при разработке ИБ

Уязвимость данных в информационной системе бухгалтерии компании обусловлена долговременным хранением большого объема данных на магнитных носителях, одновременным доступом к ресурсам нескольких пользователей. Можно выделить следующие трудности при разработке системы информационной безопасности:

* на сегодняшний день нет единой теории защищенных систем;
* производители средств защиты в основном предлагают отдельные компоненты для решения частных задач, оставляя вопросы формирования системы защиты и совместимости этих средств на усмотрение потребителей;
* для обеспечения надежной защиты необходимо разрешить целый комплекс технических и организационных проблем и разработать соответствующую документацию.

Для преодоления вышеперечисленных трудностей необходима координация действий всех участников информационного процесса. Обеспечение информационной безопасности - достаточно серьезная задача, поэтому необходимо, прежде всего, разработать концепцию безопасности информации, где определить интересы компании, принципы обеспечения и пути поддержания безопасности информации, а также сформулировать задачи по их реализации.

В основе комплекса мероприятий по информационной безопасности должна быть стратегия защиты информации. В ней определяются цели, критерии, принципы и процедуры, необходимые для построения надежной системы защиты. В разрабатываемой стратегии должны найти отражение не только степень защиты, поиск брешей, места установки брандмауэров или proxy-серверов и т. п. В ней необходимо еще четко определить процедуры и способы их применения для того, чтобы гарантировать надежную защиту.

Важнейшей особенностью общей стратегии информационной защиты является исследование системы безопасности. Можно выделить два основных направления:

* анализ средств защиты;
* определение факта вторжения.

На основе концепции безопасности информации разрабатываются стратегия безопасности информации и архитектура системы защиты информации. Следующий этап обобщенного подхода к обеспечению безопасности состоит в определении политики, содержание которой - наиболее рациональные средства и ресурсы, подходы и цели рассматриваемой задачи.

# 2.3 Анализ рисков

#

# 2.3.1 Оценка и анализ рисков ИБ

На этапе анализа рисков определяется возможность понести убытки из-за нарушения режима информационной безопасности организации, детализируются характеристики (или составляющие) рисков для информационных ресурсов и технологий. Под управлением рисками понимается процесс идентификации и уменьшения рисков, которые могут воздействовать на информационную систему.

 В простейшем случае используется оценка двух факторов: вероятность происшествия и тяжесть возможных последствий. Обычно считается, что риск тем больше, чем больше вероятность происшествия и тяжесть последствий.

Общая идея выражена формулой:

РИСК = P происшествия \* ЦЕНА ПОТЕРИ.

Определим субъективную шкалу вероятностей событий:

A − событие практически никогда не происходит;

B − событие случается редко;

C− вероятность события за рассматриваемый промежуток времени около 0,5;

D − скорее всего, событие произойдет;

E − событие почти обязательно произойдет.

Кроме того, используем субъективную шкалу серьезности происшествий.

1. N (Negligible) – Воздействием можно пренебречь.

2. Mi (Minor) – Незначительное происшествие: последствия легко устранимы, затраты на ликвидацию последствий невелики, воздействие на информационную технологию – незначительно.

3. Mo (Moderate) – Происшествие с умеренными результатами: ликвидация последствий не связана с крупными затратами, воздействие на информационную технологию не велико и не затрагивает критически важные задачи.

4. S (Serious) – Происшествие с серьезными последствиями: ликвидация последствий связана со значительными затратами, воздействие на информационные технологии ощутимо.

5. C (Critical) – Происшествие приводит к невозможности решения критически важных задач.

Для оценки рисков определяется шкала из трех значений: 1. Низкий риск.

2. Средний риск.

3. Высокий риск.

Риск, связанный с определенным событием, зависит от двух факторов и может быть определен следующим образом (табл. 8).

Таблица 8

Определение риска в зависимости от двух факторов

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Negligible | Minor | Moderate | Serious | Critical |
| A | Низкий риск | Низкий риск | Низкий риск | Средний риск | Средний риск |
| B | Низкий риск | Низкий риск | Средний риск | Средний риск | Высокий риск |
| C | Низкий риск | Средний риск | Средний риск | Средний риск | Высокий риск |
| D | Средний риск | Средний риск | Средний риск | Средний риск | Высокий риск |
| E | Средний риск | Высокий риск | Высокий риск | Высокий риск | Высокий риск |

Показатель риска измеряется в шкале от 0 до 8 со следующими определениями уровней риска:

1 − риск практически отсутствует; теоретически возможны ситуации, при которых событие наступает, но на практике это случается редко, а потенциальный ущерб сравнительно невелик;

2 − риск очень мал; события подобного рода случались достаточно редко, кроме того, негативные последствия сравнительно невелики.

8 − риск очень велик; событие скорее всего наступит, и последствия будут чрезвычайно тяжелыми и т.д.

Следующей по важности группой информации является информация по организационно – правовым вопросам (группа 2),информация по вопросам торгово-экономических отношений (группа 3) и информация по вопросам управления имуществом предприятия (группа 2). Разглашение такого рода информации конкурентам приведет к нарушению планов компании и, соответственно, повлечет за собой большие убытки. Вся остальная информация также нуждается в определенной защите, но нарушение ее безопасности приведет к устранимым последствиям.

Оценка рисков нарушения безопасности

Расходы на систему защиты информации необходимо сопоставить и привести в соответствие с ценностью защищаемой информации и других информационных ресурсов, подвергающихся риску, а также с ущербом, который может быть нанесен организации из-за сбоев в системе защиты.

Для оценки рисков необходимо систематически рассматривать следующие аспекты:

а) ущерб, который может нанести деятельности организации серьезное нарушение информационной безопасности, с учетом возможных последствий нарушения конфиденциальности, целостности и доступности информации;

б) реальная вероятность такого нарушения защиты в свете превалирующих угроз и средств контроля.

Данные бухгалтерского учета имеют первостепенное значение для деятельности любой организации, так как они формируют целостную картину финансово-хозяйственного состояния предприятия. На основании бухгалтерской отчетности осуществляются такие важнейшие функции, как планирование, оперативное управление деятельностью компании, прогнозирование, оценка состояния предприятия. Ежедневно в бухгалтерию поступает огромный поток первичных документов, которые обрабатываются бухгалтерами, вводятся в информационную систему, затем на основании первичной документации и отчетной информации предыдущего периода формируется бухгалтерская отчетность о деятельности компании в текущем периоде.

Ущерб и затраты на восстановление от повреждения, модификации и уничтожения информации напрямую зависит от временного периода, за который были уничтожены, повреждены или модифицированы данные. Чем больше временной период, тем больше ущерб и затраты на восстановление данных. Для минимизации ущерба и затрат на восстановление необходимо осуществлять резервное копирование базы данных.

# 2.3.2 Изучение и систематизация угроз ИБ

Под угрозой понимается событие (воздействие), которое в случае своей реализации становится причиной нарушения целостности информации, ее потери или замены. Угрозы могут быть как случайными, так и умышленными (преднамеренно создаваемыми).

Необходимо отметить, что зачастую ущерб наносится не из-за чьего-то злого умысла, а просто по причине элементарных ошибок пользователей, которые случайно портят или удаляют данные, жизненно важные для системы. В связи с этим, помимо контроля доступа, необходимым элементом защиты информации в компьютерных сетях является разграничение полномочий пользователей. Кроме того, вероятность ошибок обслуживающего персонала и пользователей сети может быть значительно уменьшена, если их правильно обучать и, кроме того, периодически контролировать их действия со стороны, например, администратора безопасности сети.

Трудно предсказуемыми источниками угроз информации являются аварии и стихийные бедствия. Но и в этих случаях для сохранения информации могут использоваться различные средства.

Наиболее надежное средство предотвращения потерь информации при кратковременном отключении электроэнергии - установка источников бесперебойного питания (UPS). Различные по своим техническим и потребительским характеристикам, подобные устройства могут обеспечить питание всей локальной сети или отдельного компьютера в течение времени, достаточного для восстановления подачи напряжения или для сохранения информации на магнитных носителях. Большинство UPS выполняют функции еще и стабилизатора напряжения, что является дополнительной защитой от скачков напряжения в сети. Многие современные сетевые устройства (серверы, концентраторы, мосты и др.) оснащены собственными дублированными системами электропитания.

Основной, наиболее распространенный метод защиты информации и оборудования от стихийных бедствий (пожаров, землетрясений, наводнений и т. п.) состоит в создании и хранении архивных копий данных, в том числе, в размещении некоторых сетевых устройств, например, серверов баз данных, в специальных защищенных помещениях, расположенных, как правило, в других зданиях, либо, реже, в другом районе города или в даже другом городе.

Особенностью компьютерной неосторожности является то, что безошибочных программ в принципе не бывает. Если проект практически в любой области техники можно выполнить с огромным запасом надежности, то в области программирования такая надежность весьма условна, а иногда почти не достижима. И это касается не только отдельных программ, но и целого ряда программных продуктов фирм, известных во всем мире.

Как считают эксперты по безопасности, из-за недостатков в программных продуктах Microsoft, связанных с обеспечением безопасности данных в сети Internet, хакеры могут захватывать личные ключи шифров пользователей и действовать от их лица. Поскольку существуют дефекты в некоторых программах Microsoft, включая браузер Internet Explorer и пакет Internet Information Server, ключи шифров можно легко скопировать с жестких дисков компьютеров, подключенных к WWW.

Проблема состоит в том, что форматы файлов, применяемые для защиты личных ключей шифров, до конца не проработаны. Используя лазейки в системе защиты, можно с помощью вирусного программного кода, скрытого на Web-страницах, читать содержимое жестких дисков пользователей во время посещения ими данной страницы. А из-за дефекта в программных интерфейсах криптографии, используемых многими средствами Microsoft, множество ключей могут быть считаны с жесткого диска пользователя по простому запросу. Легкость, с которой это можно выполнить, ставит под угрозу все остальные средства шифрования, применяемые на Web-страницах и в браузерах.

Уровень указанных угроз в значительной мере снижается за счет повышения квалификации обслуживающего персонала и пользователей, а также надежности аппаратно-программных и технических средств.

Однако наиболее опасным источником угроз информации являются преднамеренные действия злоумышленников. Спектр их противоправных действий достаточно широк, а итогом их вмешательства в процесс взаимодействия пользователей сети является разглашение, фальсификация, незаконное тиражирование или уничтожение конфиденциальной информации.

Стандартность архитектурных принципов построения оборудования и программ обеспечивает сравнительно легкий доступ профессионала к информации, находящейся в персональном компьютере. Ограничение доступа к ПК путем введения кодов не гарантирует стопроцентную защиту информации.

Угрозы, преднамеренно создаваемые злоумышленником или группой лиц (умышленные угрозы), заслуживают более детального анализа, так как часто носят изощренный характер и приводят к тяжелым последствиям

Обычно выделяют три основных вида угроз безопасности: угрозы раскрытия, целостности и отказа в обслуживании. Угроза раскрытия заключается в том, что информация становится известной тому, кому не следует ее знать. В терминах компьютерной безопасности угроза раскрытия имеет место всегда, когда получен доступ к некоторой конфиденциальной информации, хранящейся в вычислительной системе или передаваемой от одной системы к другой.

Нарушение конфиденциальности (раскрытие) информации - это не только несанкционированное чтение документов или электронной почты. Прежде всего, это перехват и расшифровка сетевых пакетов (как известно, информация в сети передается пакетами), другими словами, анализ трафика.

# 2.3.3 Определение каналов несанкционированного доступа

Способ несанкционированного доступа (способ НСД) - также совокупность приемов и порядок действий, но с целью получения охраняемых сведений незаконным противоправным путем и обеспечения возможности воздействовать на эту информацию (например, подменить, уничтожить и т. п.).

Существующие в настоящее время способы НСД к информации многообразны: применение специальных технических устройств, использование недостатков вычислительных систем и получение секретных сведений о защищаемых данных.

Утечка информации через технические средства может происходить, за счет:

* микрофонного эффекта элементов электронных схем;
* магнитной составляющей поля электронных схем и устройств различного назначения и исполнения;
* электромагнитного излучения низкой и высокой частоты;
* возникновения паразитной генерации усилителей различного назначения;
* наводок по цепям питания электронных систем;
* наводок по цепям заземления электронных систем;
* взаимного влияния проводов и линий связи;
* высокочастотного навязывания мощных радиоэлектронных средств и систем;

Каждый из этих каналов будет иметь структуру в зависимости от условий расположения и исполнения.

Каналы утечки информации и способы несанкционированного доступа к источникам конфиденциальной информации объективно взаимосвязаны. Каждому каналу соответствует определенный способ НСД.

Вариант взаимосвязи способов несанкционированного доступа к объектам и источникам охраняемой информации и каналов утечки конфиденциальной информации приведен в табл. 10.

Таблица 10

|  |  |
| --- | --- |
| Способнесанкционированногодоступа | Тип канала утечки информации |
| Визуальный | Акустический | Электромагнитный(магнитный,электрический) | Материально-вещественные |
| Подслушивание |  | + | + |  |
| Визуальное наблюдение | + |  |  |  |
| Хищение |  |  | + | + |
| Копирование |  |  | + | + |
| Подделка |  |  | + | + |
| Незаконное подключение |  | + | + |  |
| Перехват |  | + | + |  |
| Фотографирование | + |  |  |  |
| Итого по виду канала | 2 | 3 | 6 | 3 |

Способы НСД к проводным линиям связи.

Наиболее часто для передачи информации применяются телефонные линии в качестве проводных линий связи. Это связано с тем, что большинство компьютеров используют для передачи данных модемы, подключенные к телефонной линии.

Общепринятые способы подслушивания линии, связывающей компьютеры:

* непосредственное подключение к телефонной линии:
* контактное - последовательное или параллельное (прямо на АТС или где-нибудь на линии между телефонным аппаратом и АТС);
* бесконтактное (индукционное) подключение к телефонной линии;
* помещение радиоретранслятора («жучка») на телефонной линии:
* последовательное включение;

#

# 2.3.4 Оценка состояния информационной безопасности в ООО магазин «Стиль»

Завершающим этапом предпроектного обследования является оценка состояния информационной безопасности в организации.

Решение данной задачи основывается на анализе сведений, полученных на этапе информационного обследования ИС.

Целью этапа является анализ соответствия уровня нормативного и организационно-технического обеспечения информационной безопасности объекта аудита установленным требованиям руководящих документов Гостехкомиссии при Президенте РФ, типовым требованиям международных стандартов ISO и соответствующим требованиям компании-заказчика. К первой области также относятся работы, проводимые на основе анализа рисков, инструментальные исследования (исследование элементов инфраструктуры компьютерной сети и корпоративной информационной системы на наличие уязвимостей, исследование защищенности точек доступа в Internet). Данный комплекс работ также включает в себя анализ документооборота, который, в свою очередь, можно выделить и как самостоятельное направление.

Рассмотрим инструментальный анализ защищённости АС, направленный на выявление и устранение уязвимостей программно-аппаратного обеспечения системы.

Инструментальный анализ представляет собой чаще всего сбор информации о состоянии системы сетевой защиты с помощью специального программного обеспечения и специальных методов. Под состоянием системы сетевой защиты понимаются лишь те параметры и настройки, использование которых помогает злоумышленнику проникнуть в сети и нанести урон предприятию. В процессе проведения инструментального анализа защищенности моделируется как можно большее количество таких сетевых атак, которые может выполнить злоумышленник.

Результатом является информация обо всех уязвимостях, степени их критичности и методах устранения, сведения о широкодоступной информации (информации, доступной любому потенциальному нарушителю) сети заказчика.

По завершении инструментального анализа выдаются рекомендации по модернизации системы сетевой защиты, которые позволяют устранить опасные уязвимости и тем самым повысить уровень защищенности ИС от действий злоумышленника при минимальных затратах на ИБ.

Результаты тестирования на соответствие ГОСТ Р ИСО/МЭК 17799–2005 представлены на рис. 6.

Рис. 6. Определение степени соответствия требованиям стандарта

Информация, полученная по результатам комплексной оценки, является отправной точкой для принятия руководителями управленческих решений, способствующих повышению защищенности информационных ресурсов.

# 2.4 Определение класса защищенности системы и показателей защищенности от несанкционированного доступа

Коммерческая тайна — режим конфиденциальности информации, позволяющий её обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду. Защищаемая информация на предприятии не может быть отнесена к разряду коммерческой тайны. Исходя из этого, можно определить четвертый класс защищенности системы.

# 2.4.1 Определение требований к информационной безопасности

Данные бухгалтерского учета в виде всевозможных отчетов сохраняются длительное время, причем как в электронном, так и бумажном виде. Информация о состоянии финансово-хозяйственной деятельности предприятия в текущем периоде может быть получена только при наличии аналогичной информации за предшествующий период, поэтому потеря, порча и модификация этой информации может причинить немалый вред компании. В рамках информационной безопасности для нормального функционирования механизмов бухгалтерского учета необходимо обеспечить целостность и полноту базы данных, предотвращение потери и некорректного изменения информации в базе данных.

Каждый сбой работы базы данных − это не только моральный ущерб для работников предприятия и сетевых администраторов. По мере развития технологий электронных платежей, «безбумажного» документооборота и серьезный сбой локальных сетей может парализовать работу компании, что приведет к ощутимым убыткам. При этом защита данных в компьютерных сетях становится одной из самых острых проблем.

Для данной информации необходимо обеспечить выполнение всех трех критериев обеспечения безопасности:

* конфиденциальность — доступность информации только определённому кругу лиц;
* целостность — гарантия существования информации в исходном виде;
* доступность — возможность получение информации авторизованным пользователем в нужное для него время.

Это обусловлено тем, что потеря, несанкционированная модификация или разглашение информации из данных баз может повлечь за собой тяжелые последствия в виде убытков, временных остановок деятельности предприятия и др.

Также необходимо обеспечить целостность и доступность поступающих данных от поставщиков комплектующих: цен и перечня доступных товаров для закупки. Недоступность данной информации может привести к остановке выполнения оптовых заказов клиентов, что негативно скажется на работе предприятия.

Целостность данных необходимо гарантировать для отчетности и платежных поручений, отправляемых посредством сети Интернет.

Требования к показателям четвертого класса защищенности:

1. Дискреционный принцип контроля доступа.

Комплекс средств защиты (КСЗ) должен контролировать доступ наименованных субъектов (пользователей) к наименованным объектам (файлам, программам, томам и т.д.). Для каждой пары (субъект – объект) в средствах вычислительной техники (СВТ) должно быть задано явное и недвусмысленное перечисление допустимых типов доступа (читать, писать и т.д.), т.е. тех типов доступа, которые являются санкционированными для данного субъекта (индивида или группы индивидов) к данному ресурсу СВТ (объекту). Должны быть предусмотрены средства управления, ограничивающие распространение прав на доступ. Контроль доступа должен быть применим к каждому объекту и каждому субъекту (индивиду или группе равноправных индивидов). Механизм, реализующий дискреционный принцип контроля доступа, должен предусматривать возможности санкционированного изменения правил разграничения доступа (ПРД), в том числе возможность санкционированного изменения списка пользователей СВТ и списка защищаемых объектов. Права изменять ПРД должны предоставляться выделенным субъектам (администрации, службе безопасности и т.д.).

Дополнительно КСЗ должен содержать механизм, претворяющий в жизнь дискреционные ПРД, как для явных действий пользователя, так и для скрытых, обеспечивая тем самым защиту объектов от НСД (т.е. от доступа, не допустимого с точки зрения заданного ПРД). Под "явными" здесь подразумеваются действия, осуществляемые с использованием системных средств - системных макрокоманд, инструкций языков высокого уровня и т.д., а под "скрытыми" - иные действия, в том числе с использованием собственных программ работы с устройствами.

Дискреционные ПРД для систем данного класса являются дополнением мандатных ПРД.

2. Мандатный принцип контроля доступа.

Для реализации этого принципа должны сопоставляться классификационные метки каждого субъекта и каждого объекта, отражающие их место в соответствующей иерархии. Посредством этих меток субъектам и объектам должны назначаться классификационные уровни (уровни уязвимости, категории секретности и т.п.), являющиеся комбинациями иерархических и не иерархических категорий. Данные метки должны служить основой мандатного принципа разграничения доступа.

КСЗ при вводе новых данных в систему должен запрашивать и получать от санкционированного пользователя классификационные метки этих данных. При санкционированном занесении в список пользователей нового субъекта должно осуществляться сопоставление ему классификационных меток. Внешние классификационные метки (субъектов, объектов) должны точно соответствовать внутренним меткам (внутри КСЗ).

КСЗ должен реализовывать мандатный принцип контроля доступа применительно ко всем объектам при явном и скрытом доступе со стороны любого из субъектов:

* субъект может читать объект, только если иерархическая классификация в классификационном уровне субъекта не меньше, чем иерархическая классификация в классификационном уровне объекта, и не иерархические категории в классификационном уровне субъекта включают в себя все иерархические категории в классификационном уровне объекта;
* субъект осуществляет запись в объект, только если классификационный уровень субъекта в иерархической классификации не больше, чем классификационный уровень объекта в иерархической классификации, и все иерархические категории в классификационном уровне субъекта включаются в неиерархические категории в классификационном уровне объекта.

Реализация мандатных ПРД должна предусматривать возможности сопровождения: изменения классификационных уровней субъектов и объектов специально выделенными субъектами.

В СВТ должен быть реализован диспетчер доступа, т.е. средство, осуществляющее перехват всех обращений субъектов к объектам, а также разграничение доступа в соответствии с заданным принципом разграничения доступа. При этом решение о санкционированности запроса на доступ должно приниматься только при одновременном разрешении его и дискреционными, и мандатными ПРД. Таким образом, должен контролироваться не только единичный акт доступа, но и потоки информации.

3. Очистка памяти.

При первоначальном назначении или при перераспределении внешней памяти КСЗ должен затруднять субъекту доступ к остаточной информации. При перераспределении оперативной памяти КСЗ должен осуществлять ее очистку.

4. Изоляция модулей.

При наличии в СВТ мультипрограммирования в КСЗ должен существовать программно-технический механизм, изолирующий программные модули одного процесса (одного субъекта), от программных модулей других процессов (других субъектов) - т.е. в оперативной памяти ЭВМ программы разных пользователей должны быть защищены друг от друга.

5. Маркировка документов.

При выводе защищаемой информации на документ в начале и конце проставляют штамп № 1 и заполняют его реквизиты в соответствии с Инструкцией № 0126-87.

6. Защита ввода и вывода на отчуждаемый физический носитель информации.

КСЗ должен различать каждое устройство ввода-вывода и каждый канал связи как произвольно используемые или идентифицированные ("помеченные"). При вводе с "помеченного" устройства (вывода на "помеченное" устройство) КСЗ должен обеспечивать соответствие между меткой вводимого (выводимого) объекта (классификационным уровнем) и меткой устройства. Такое же соответствие должно обеспечиваться при работе с "помеченным" каналом связи.

Изменения в назначении и разметке устройств и каналов должны осуществляться только под контролем КСЗ.

7. Сопоставление пользователя с устройством.

КСЗ должен обеспечивать вывод информации на запрошенное пользователем устройство как для произвольно используемых устройств, так и для идентифицированных (при совпадении маркировки).

Идентифицированный КСЗ должен включать в себя механизм, посредством которого санкционированный пользователь надежно сопоставляется выделенному устройству.

8. Идентификация и аутентификация.

КСЗ должен требовать от пользователей идентифицировать себя при запросах на доступ, должен проверять подлинность идентификатора субъекта — осуществлять аутентификацию. КСЗ должен располагать необходимыми данными для идентификации и аутентификации и препятствовать входу в СВТ неидентифицированного пользователя или пользователя, чья подлинность при аутентификации не подтвердилась.

КСЗ должен обладать способностью надежно связывать полученную идентификацию со всеми действиями данного пользователя.

9. Регистрация.

КСЗ должен быть в состоянии осуществлять регистрацию следующих событий:

* использование идентификационного и аутентификационного механизма;
* запрос на доступ к защищаемому ресурсу (открытие файла, запуск программы и т.д.);
* создание и уничтожение объекта;
* действия по изменению ПРД.

Для каждого из этих событий должна регистрироваться следующая информация:

* дата и время;
* субъект, осуществляющий регистрируемое действие;
* тип события (если регистрируется запрос на доступ, то следует отмечать объект и тип доступа);
* успешно ли осуществилось событие (обслужен запрос на доступ или нет).

КСЗ должен содержать средства выборочного ознакомления с регистрационной информацией.

Дополнительно должна быть предусмотрена регистрация всех попыток доступа, всех действий оператора и выделенных пользователей (администраторов защиты и т.п.).

10. Целостность КСЗ.

В СВТ четвертого класса защищенности должен осуществляться периодический контроль за целостностью КСЗ.

Программы КСЗ должны выполняться в отдельной части оперативной памяти.

11. Тестирование.

В четвертом классе защищенности должны тестироваться:

* реализация ПРД (перехват запросов на доступ, правильное распознавание санкционированных и несанкционированных запросов в соответствии с дискреционными и мандатными правилами, верное сопоставление меток субъектов и объектов, запрос меток вновь вводимой информации, средства защиты механизма разграничения доступа, санкционированное изменение ПРД);
* невозможность присвоения субъектом себе новых прав;
* очистка оперативной и внешней памяти;
* работа механизма изоляции процессов в оперативной памяти;
* маркировка документов;
* защита вода и вывода информации на отчуждаемый физический носитель и сопоставление пользователя с устройством;
* идентификация и аутентификация, а также их средства защиты;
* запрет на доступ несанкционированного пользователя;
* работа механизма, осуществляющего контроль за целостностью СВТ;
* регистрация событий, средства защиты регистрационной информации и возможность санкционированного ознакомления с этой информацией.

12. Руководство для пользователя.

Документация на СВТ должна включать в себя краткое руководство для пользователя с описанием способов использования КСЗ и его интерфейса с пользователем.

13. Руководство по КСЗ.

Данный документ адресован администратору защиты и должен содержать:

* описание контролируемых функций;
* руководство по генерации КСЗ;
* описания старта СВТ, процедур проверки правильности старта, процедур работы со средствами регистрации.

14. Тестовая документация.

Должно быть представлено описание тестов и испытаний, которым подвергалось СВТ и результатов тестирования.

# 2.4.2 Модель потенциального нарушителя

Потенциальных нарушителей системы безопасности 2:

1. неквалифицированный (или враждебно настроенный) работник;
2. внешний по отношению к организации злоумышленник.

Оба типа нарушителей столкнутся с меньшим уровнем защиты в дневное время суток, т.к. для сотрудника вход на рабочее место является свободным, а для внешнего злоумышленника существует потенциальная возможность войти в систему через Интернет.

Наиболее вероятным нарушителем выступает сотрудник компании, т.к. ему не придется преодолевать уровни защиты от внешних злоумышленников. Даже неумышленные (возможно, ошибочные) действия сотрудника с высоким уровнем доступа к информации может серьезно повредить систему и затормозить, а иногда даже полностью остановить работу компании.

Маловероятно, что квалификация сотрудника как умышленного нарушителя информационной безопасности будет очень высокой. Скорее всего, это будет уровень начинающего взломщика или просто продвинутого пользователя ПК.

Хоть и маловероятен, но теоретически возможны попытки взлома из внешней среды через подключение к Интернет. В данном случае также не предполагается высокая квалификация потенциального нарушителя, т. к. информация, хранящаяся на сервере не составляет коммерческой тайны.

Основным мотивом действий того и другого типа нарушителей может быть попытка вредительства компании в качестве мести (в случае сотрудника), ради развлечения или по заказу конкурентов (в случае внешнего злоумышленника). Заказ конкурентов мало вероятен, но даже в случае реализации данной угрозы конкуренты не будут нанимать высококвалифицированного специалиста, т.к. преодолеть физическую защиту будет намного дешевле.

# 3. Проектирование системы информационной безопасности отдела бухгалтерии ООО магазин «Стиль»

# 3.1 Рекомендации по разработке концепции информационной безопасности ООО магазин «Стиль»

Концепция информационной безопасности организации − это:

– во-первых, это нормативный документ, на основании которого будет строиться ИБ организации;

– во-вторых, это решение проблемы информационной безопасности в организации;

– в-третьих, этот документ опирается на нормативную базу Российского законодательства, моральные нормы, научно-технические принципы и организационные возможности.

Концепция информационной безопасности для организации должна состоять из следующих разделов:

1. Введение

Настоящая Концепция определяет систему взглядов на проблему обеспечения безопасности информации в организации и представляет собой систематизированное изложение целей и задач защиты, а также принципов и способов достижения требуемого уровня безопасности информации.

При построении системы безопасности информационных ресурсов организация основывается на комплексном подходе, доказавшем свою эффективность и надежность. Комплексный подход ориентирован на создание защищенной среды обработки информации, сводящей воедино разнородные меры противодействия угрозам. Сюда относятся правовые, морально-этические, организационные, программные и технические способы обеспечения информационной безопасности.

Правовой базой для разработки настоящей концепции служат требования действующих в России законодательных и нормативных документов.

Концепция является методологической основой для формирования и проведения в организации единой политики в области обеспечения безопасности информации (политики безопасности), для принятия управленческих решений и разработки практических мер по ее воплощению.

2. Общие положения

В данном разделе концепции дано название и правовая основа данного документа, т.е. необходимо дать понять, что подразумевается под словом «концепция» в данном документе, какова система взглядов на проблему безопасности.

В концепции должно быть учтено современное состояние, и ближайшие перспективы развития системы информационной безопасности. Также описывается, на какие объекты информационной системы она распространяется, и для чего будет являться методологической основой. В завершении данного раздела необходимо указать, какие принципы были положены в основу построения системы информационной безопасности.

3. Объекты защиты

В данном разделе концепции необходимо указать основные объекты, на которые направлена информационная безопасность в организации:

- информационные ресурсы с ограниченным доступом, составляющие коммерческую, банковскую тайну, иные чувствительные по отношению к случайным и несанкционированным воздействиям и нарушению их безопасности информационные ресурсы, в том числе открытая (общедоступная) информация, представленные в виде документов и массивов информации, независимо от формы и вида их представления;

- процессы обработки информации, информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации, научно-технический персонал разработчиков и пользователей системы и ее обслуживающий персонал;

- информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены чувствительные компоненты АС.

4. Основные угрозы

В этом разделе необходимо описать модель возможного нарушителя, рассмотреть различные возможности утечки информации по техническим каналам, дать определение умышленным действиям различными лицами, указать, какие пути могут быть для реализации неправомерных действий и какие вообще могут быть угрозы безопасности информации и ее источники.

5. Основные положения технической политики в обеспечении безопасности информации

Реализация технической политики по обеспечению информационной безопасности в организации должна исходить из того, что нельзя обеспечить требуемый уровень безопасности только одним мероприятием или средством, а необходим комплексный подход с системным согласованием различных элементов, а каждый разработанный элемент должен рассматриваться как часть единой системы при оптимальном соотношении как технических средств, так и организационных мероприятий.

Должны быть перечислены основные направления технической политики и то, как она будет осуществляться.

Также необходимо формирование режима безопасности информации, т.е. согласно выявленным угрозам режим защиты формируется как совокупность способов и мер защиты информации. Комплекс мер по формированию режима безопасности информации должен включать в себя: организационно-правовой режим (нормативные документы), организационно-технические мероприятия (аттестация рабочих мест), программно-технические мероприятия, комплекс мероприятий по контролю за функционированием АС и систем ее защиты, комплекс оперативных мероприятий по предотвращению несанкционированного доступа, а также комплекс действий по выявлению таких попыток.

6. Принципы построения комплексной системы защиты

Построение системы безопасности информации АС и ее функционирование должны осуществляться в соответствии со следующими принципами:

* законность: предполагает осуществление защитных мероприятий и разработку системы безопасности информации АС организации в соответствии с действующим законодательством;
* системность: системный подход к построению системы защиты информации предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенных для понимания и решения проблемы обеспечения безопасности информации;
* комплексность: комплексное использование методов и средств защиты компьютерных систем предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов;
* непрерывность защиты: непрерывный, целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла АС;
* своевременность: предполагает упреждающий характер мер для обеспечения безопасности информации;
* преемственность и совершенствование: предполагают постоянное совершенствование мер и средств защиты информации;
* разумная достаточность (экономическая целесообразность): предполагает соответствие уровня затрат на обеспечение безопасности информации ценности информационных ресурсов и величине возможного ущерба;
* персональная ответственность: предполагает возложение ответственности за обеспечение безопасности информации и системы ее обработки на каждого сотрудника в пределах его полномочий;
* принцип минимизации полномочий: означает предоставление пользователям минимальных прав доступа в соответствии с производственной необходимостью;
* взаимодействие и сотрудничество: предполагает создание благоприятной атмосферы в коллективах подразделений;
* гибкость системы защиты: для обеспечения возможности варьирования уровня защищенности средства защиты должны обладать определенной гибкостью;
* открытость алгоритмов и механизмов защиты: суть данного принципа состоит в том, что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможности ее преодоления (даже авторам), однако это не означает, что информация о конкретной системе защиты должна быть общедоступна;
* простота применения средств защиты: механизм защиты должен быть интуитивно понятен и прост в использовании, без значительных дополнительных трудозатрат;
* научная обоснованность и техническая реализуемость: информационные технологии, технические и программные средства, средства и меры защиты информации должны быть реализованы на современном уровне развития науки и техники, научно обоснованы с точки зрения достижения заданного уровня безопасности информации и должны соответствовать установленным нормам и требованиям по безопасности информации;
* специализация и профессионализм: предполагает привлечение к разработке средств и реализаций мер защиты информации специализированных организаций, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области, реализация административных мер и эксплуатация средств защиты должна осуществляться профессионально подготовленными специалистами;
* обязательность контроля: предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил безопасности.

7. Первоочередные мероприятия

В данном разделе необходимо описать первоочередные действия, которые предстоит исполнить в ближайшее время, описать аппаратно-программный комплекс, который обеспечит информационную безопасность организации.

# 3.2 Разработка политики ИБ и выбор решений по обеспечению политики ИБ

В основе организационных мер защиты информации лежит политика безопасности, от эффективности которой в наибольшей степени зависит успешность мероприятий по обеспечению информационной безопасности.

Под политикой информационной безопасности 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 безопасности строится на основе анализа рисков. С учетом рисков, выявленных в организации, политика информационной безопасности для организации должна содержать семь разделов:

-«Введение». Необходимость появления политики безопасности на основании выявленных недостатков в информационной безопасности ООО «Стиль»;

-«Цель политики». В этом разделе документа для ООО «Стиль» необходимо отразить цели создания данного документа (в частности, для парольной политики – «установление стандартов для создания «сильных» паролей, их защиты и регулярной смены»);

-«Область применения». В данном разделе необходимо описать объекты или субъекты ООО «Стиль», которые должны выполнять требования данной политики (например, «данная политика применяется ко всем сотрудникам, имеющим любую форму доступа к любым информационным ресурсам компании»);

-«Политика». В данном разделе необходимо описать сами требования к информационной безопасности (например, парольная политика должна содержать пять подразделов: «Создание паролей», «Изменение паролей», «Защита паролей», «Использование паролей при разработке приложений», «Использование паролей при удаленном доступе»);

-«Ответственность». Описывает наказание за нарушение указанных в предыдущем разделе требований;

-«История изменений данной политики». Дает возможность отследить все вносимые в документ изменения (дата, автор, краткая суть изменения).

Такая структура позволит лаконично описать все основные моменты, связанные с предметом политики безопасности организации, не «привязываясь» к конкретным техническим решениям, продуктам и производителям. Иначе изменение политической ситуации в компании и т. п. приведет к необходимости изменения концепции ИБ, а этого происходить не должно.

Кроме того, в политике безопасности организации должны быть определены обязанности должностных лиц по выработке программы безопасности и проведению ее в жизнь. В этом смысле политика безопасности является основой подотчетности персонала.

# 3.2.1 Административный уровень ИБ

К административному уровню информационной безопасности относятся действия общего характера, предпринимаемые руководством организации.

Главная цель мер административного уровня - сформировать программу работ в области информационной безопасности и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

Основой программы является политика безопасности, отражающая подход организации к защите своих информационных активов. Руководство компании должно осознать необходимость поддержания режима безопасности и выделения на эти цели значительных ресурсов, а также назначить ответственных за разработку, внедрение и сопровождение системы безопасности. Для ООО «Стиль» актуальным является создание службы информационной безопасности в составе 3 человек, которые будут отвечать за разработку, внедрение и совершенствование системы безопасности.

С практической точки зрения политику безопасности целесообразно рассматривать на трех уровнях детализации. К верхнему уровню можно отнести решения, затрагивающие организацию в целом. Они носят весьма общий характер и исходят от руководства организации. Список решений этого уровня включает в себя следующие элементы:

* решение сформировать или пересмотреть комплексную программу обеспечения информационной безопасности, назначение ответственных за продвижение программы;
* формулировка целей, которые преследует организация в области информационной безопасности, определение общих направлений в достижении этих целей;
* обеспечение базы для соблюдения законов и правил;
* формулировка административных решений по тем вопросам реализации программы безопасности, которые должны рассматриваться на уровне организации в целом.

Для политики верхнего уровня цели организации в области информационной безопасности формулируются в терминах целостности, доступности и конфиденциальности. Так как компания отвечает за поддержание критически важной базы данных бухгалтерии, то на первом плане стоит задача уменьшение числа потерь, повреждений или искажений данных.

На верхний уровень выносится управление защитными ресурсами и координация использования этих ресурсов, выделение специального персонала для защиты критически важных систем и взаимодействие с другими организациями, обеспечивающими или контролирующими режим безопасности.

Политика верхнего уровня имеет дело с тремя аспектами законопослушности и исполнительской дисциплины. Во-первых, организация должна соблюдать существующие законы. Во-вторых, следует контролировать действия лиц, ответственных за выработку программы безопасности. Наконец, необходимо обеспечить определенную степень исполнительности персонала, а для этого нужно выработать систему поощрений и наказаний.

Вообще говоря, на верхний уровень следует выносить минимум вопросов. Подобное вынесение целесообразно, когда оно сулит значительную экономию средств или когда иначе поступить просто невозможно.

В документ, характеризующий политику безопасности компании необходимо включить следующие разделы:

* вводный, подтверждающий озабоченность высшего руководства проблемами информационной безопасности;
* организационный, содержащий описание подразделений, комиссий, групп и т.д., отвечающих за работы в области информационной безопасности;
* классификационный, описывающий имеющиеся в организации материальные и информационные ресурсы и необходимый уровень их защиты;
* штатный, характеризующий меры безопасности, применяемые к персоналу (описание должностей с точки зрения информационной безопасности, организация обучения и переподготовки персонала, порядок реагирования на нарушения режима безопасности и т.п.);
* раздел, освещающий вопросы физической защиты;
* управляющий раздел, описывающий подход к управлению компьютерами и компьютерными сетями;
* раздел, описывающий правила разграничения доступа к производственной информации;
* раздел, характеризующий порядок разработки и сопровождения систем;
* раздел, описывающий меры, направленные на обеспечение непрерывной работы организации;
* юридический раздел, подтверждающий соответствие политики безопасности действующему законодательству.

К административным мероприятиям защиты, необходимым для проведения в бухгалтерии торговой компании, относятся:

* поддержка правильной конфигурации ОС;
* создание, ведение и контроль журналов работы пользователей в ИС с помощью встроенных механизмов программы 1С: Бухгалтерия 7.7;
* выявление «брешей» в системе защиты;
* проведение тестирования средств защиты;
* контроль смены паролей.

# 3.2.2 Организационный уровень ИБ

К организационным средствам защиты можно отнести организационно-технические и организационно-правовые мероприятия, осуществляемые в процессе создания и эксплуатации ИС с целью обеспечения защиты информации. Организационные мероприятия охватывают все структурные элементы ИС и системы защиты на всех этапах их жизненного цикла. При этом организационные мероприятия играют двоякую роль в механизме защиты: с одной стороны, позволяют полностью или частично перекрывать значительную часть каналов утечки информации, а с другой – обеспечивают объединение всех используемых в ИС средств в целостный механизм защиты.

Организационные меры защиты базируются на законодательных и нормативных документах по безопасности информации. Они должны охватывать все основные пути сохранения информационных ресурсов и включать:

* ограничение физического доступа к объектам ИС и реализацию режимных мер;
* ограничение возможности перехвата информации вследствие существования физических полей;
* ограничение доступа к информационным ресурсам и другим элементам ИС путем установления правил разграничения доступа, криптографическое закрытие каналов передачи данных, выявление и уничтожение «закладок»;
* создание твердых копий важных с точки зрения утраты массивов данных;
* проведение профилактических и других мер от внедрения вирусов.

К организационно-правовым мероприятиям защиты, необходимыми для проведения в бухгалтерии ООО «Стиль» относятся:

* организация и поддержание надежного пропускного режима и контроль посетителей;
* надежная охрана помещений компании и территории;
* организация защиты информации, т. е. назначение ответственного за защиту информации, проведение систематического контроля за работой персонала, порядок учета, хранения и уничтожения документов;

Организационные мероприятия при работе с сотрудниками компании включают в себя:

* беседы при приеме на работу;
* ознакомление с правилами и процедурами работы с ИС на предприятии;
* обучение правилам работы с ИС для сохранения ее целостности и корректности данных;
* беседы с увольняемыми.

В результате беседы при приеме на работу устанавливается целесообразность приема кандидата на соответствующую вакансию.

Обучение сотрудников предполагает не только приобретение и систематическое поддержание на высоком уровне производственных навыков, но и психологическое их воспитание в глубокой убежденности, что необходимо выполнять требования промышленной (производственной) секретности, информационной безопасности. Систематическое обучение способствует повышению уровня компетентности руководства и сотрудников в вопросах защиты коммерческих интересов своего предприятия. Беседы с увольняющимися имеют главной целью предотвратить разглашение информации или ее неправильное использование. В ходе беседы следует особо подчеркнуть, что каждый увольняющийся сотрудник имеет твердые обязательства о неразглашении фирменных секретов и эти обязательства, как правило, подкрепляются подпиской о неразглашении известных сотруднику конфиденциальных сведений.

Организационно-технические меры защиты включают следующие основные мероприятия:

* резервирование (наличие всех основных компонентов операционной системы и программного обеспечения в архивах, копирование таблиц распределения файлов дисков, ежедневное ведение архивов изменяемых файлов);
* профилактика (систематическая выгрузка содержимого активной части винчестера на дискеты, раздельное хранение компонентов программного обеспечения и программ пользователей, хранение неиспользуемых программ в архивах);
* ревизия (обследование вновь получаемых программ на дискетах и дисках на наличие вирусов, систематическая проверка длин файлов, хранящихся на винчестере, использование и постоянная проверка контрольных сумм при хранении и передаче программного обеспечения, проверка содержимого загрузочных секторов винчестера и используемых дискет системных файлов);
* фильтрация (разделение винчестера на логические диски с различными возможностями доступа к ним, использование резидентных программных средств слежения за файловой системой);

Все эти мероприятия, в той или иной степени, включают использование различных программных средств защиты. К их числу необходимо отнести программу-архиватор WinRar, программы резервирования важных компонентов файловой системы, просмотра содержимого файлов и загрузочных секторов, подсчета контрольных сумм и собственно программ защиты. Резервирование данных ИС должно проводиться с использованием встроенных средств программы 1С Бухгалтерия 7.7.

# 3.2.3 Технический уровень ИБ

Инженерно-техническое обеспечение безопасности информации путем осуществления необходимых технических мероприятий должно исключать:

* неправомочный доступ к аппаратуре обработки информации путем контроля доступа в помещении бухгалтерии;
* неправомочный вынос носителей информации персоналом, занимающимся обработкой данных, посредством выходного контроля;
* несанкционированное введение данных в память, изменение или стирание информации, хранящейся в памяти;
* неправомочное пользование системами обработки информации и незаконное получение в результате этого данных;
* доступ в системы обработки информации посредством самодельных устройств и незаконное получение данных;
* возможность неправомочной передачи данных через компьютерную сеть;
* бесконтрольный ввод данных в систему;
* неправомочное считывание, изменение или стирание данных в процессе их передачи или транспортировки носителей информации.

Инженерно-техническая защита использует следующие средства:

* физические средства;
* аппаратные средства;
* программные средства;

Методы защиты информации от большинства угроз базируются на инженерных и технических мероприятиях. Инженерно-техническая защита - это совокупность специальных органов, технических средств и мероприятий, функционирующих совместно для выполнения определенной задачи по защите информации.

Для построения системы физической безопасности необходимы следующие средства

* аппаратура тревожной сигнализации, обеспечивающая обнаружение попыток проникновения и несанкционированных действий, а также оценку их опасности;
* системы связи, обеспечивающие сбор, объединение и передачу тревожной информации и других данных (для этой цели подойдет организация офисной АТС);
* персонал охраны, выполняющий ежедневные программы безопасности, управление системой и ее использование в нештатных ситуациях.

К инженерным мероприятиям, необходимым для проведения в бухгалтерии ООО «Стиль», относятся:

* защита акустического канала;
* экранирование помещения бухгалтерии.

К аппаратным средствам относятся приборы, устройства, приспособления и другие технические решения, используемые в интересах обеспечения безопасности.

В бухгалтерии необходимо:

* в терминалах пользователей размещать устройства, предназначенные для предупреждения несанкционированного включения терминала в работу (блокираторы);
* обеспечить идентификацию терминала (схемы генерирования идентифицирующего кода);
* обеспечить идентификацию пользователя (магнитные индивидуальные карточки).

Программные средства - это специальные программы, программные комплексы и системы защиты информации в информационных системах различного назначения и средствах обработки данных.

К задачам программных средств защиты относятся:

* идентификация и аутентификация;
* управление доступом;
* обеспечение целостности и сохранности данных;
* контроль субъектов взаимодействия;
* регистрация и наблюдение.

#

# **3.3. Создание системы информационной безопасности**

#

# **3.3.1 Разработка структуры системы**

В соответствии с выделенными требованиями система информационной безопасности бухгалтерии ООО «Стиль» должна включать в себя следующие подсистемы:

* подсистему идентификации и аутентификации пользователей;
* подсистему защиты от вредоносного программного обеспечения;
* подсистему резервного копирования и архивирования;
* подсистема защиты информации в ЛВС;
* подсистема обеспечения целостности данных;
* подсистема регистрации и учета;
* подсистема обнаружения сетевых атак.

# 3.3.2 Подсистема идентификации и аутентификации пользователей

Предотвратить ущерб, связанный с утратой хранящейся в компьютерах данных бухгалтерского учета, - одна из важнейших задач для бухгалтерии компании. Известно, что персонал предприятия нередко оказывается главным виновником этих потерь. Каждый сотрудник должен иметь доступ только к своему рабочему компьютеру во избежание случайной или преднамеренной модификации, изменения, порчи или уничтожения данных.

Основным способом защиты информации считается внедрение так называемых средств ААА, или 3А (authentication, authorization, administration - аутентификация, авторизация, администрирование). Среди средств ААА значимое место занимают аппаратно-программные системы идентификации и аутентификации (СИА) к компьютерам.

При использовании СИА сотрудник получает доступ к компьютеру или в корпоративную сеть только после успешного прохождения процедуры идентификации и аутентификации. Идентификация заключается в распознавании пользователя по присущему или присвоенному ему идентификационному признаку. Проверка принадлежности пользователю предъявленного им идентификационного признака осуществляется в процессе аутентификации.

Современные СИА по виду используемых идентификационных признаков разделяются на электронные, биометрические и комбинированные (см. рис. 7).

Рис. 7. Классификация СИА по виду идентификационных признаков

В бухгалтерии планируется использование систему идентификации и аутентификации Rutoken.

Rutoken RF - это usb-токен со встроенной радиочастотной меткой (RFID-меткой). Он предназначен для доступа пользователей к информационным ресурсам компьютера и для физического доступа в здания и помещения.

РУТОКЕН RF объединяет возможности, предоставляемые usb-токенами, смарт-картами и бесконтактными электронными пропусками:

* строгая двухфакторная аутентификация при доступе к компьютеру и к защищенным информационным ресурсам;
* безопасное хранение криптографических ключей и цифровых сертификатов;
* применение в системах контроля и управления доступом, в системах учета рабочего времени и аудита перемещений сотрудников;
* использование в виде пропуска для электронных проходных.

Электронный идентификатор РУТОКЕН это небольшое устройство, подключаемое к USB-порту компьютера. РУТОКЕН является аналогом смарт-карты, но для работы с ним не требуется дополнительное оборудование (считыватель).

РУТОКЕН предназначен для аутентификации пользователей при доступе к информации и различным системам, безопасного хранения паролей, ключей шифрования, цифровых сертификатов. РУТОКЕН способен решать проблемы авторизации и разделения доступа в сетях, контролировать доступ к защищённым информационным ресурсам, обеспечивать необходимый уровень безопасности при работе с электронной почтой, хранить пароли и ключи шифрования .

В РУТОКЕН реализована файловая система организации и хранения данных по ISO 7816. Токен поддерживает стандарты PS/CS и PKCS#11. Это позволит быстро встроить поддержку РУТОКЕН, как в новые, так и в уже существующие приложения.

РУТОКЕН используется для решения следующих задач:

Аутентификация

* Замена парольной защиты при доступе к БД, VPN-сетям и security-ориентированным приложениям на программно-аппаратную аутентификацию.
* Шифрование соединений при доступе к почтовым серверам, серверам баз данных, Web-серверам, файл-серверам, аутентификация при удалённом администрировании.

Защита данных

* Защита электронной почты (ЭЦП, шифрование).
* Защита доступа к компьютеру (авторизация пользователя при входе в операционную систему).

РУТОКЕН может выступать как единое идентификационное устройство для доступа пользователя к разным элементам корпоративной системы и обеспечивать, необходимое разграничение доступа, автоматическую цифровую подпись создаваемых документов, аутентификация при доступе к компьютерам и приложениям системы.

## Технические характеристики:

* базируется на защищенном микроконтроллере;
* интерфейс USB (USB 1.1 / USB 2.0);
* EEPROM память 8, 16, 32, 64 и 128 Кбайт;
* 2-факторная аутентификация (по факту наличия РУТОКЕН и по факту предъявления PIN-кода);
* 32-битовый уникальный серийный номер;
* поддержка стандартов:
	+ ISO/IEC 7816;
	+ PC/SC;
	+ ГОСТ 28147-89;
	+ Microsoft Crypto API и Microsoft Smartcard API;
	+ PKCS#11 (v. 2.10+).

Бесконтактный пропуск для выхода из помещения и средство доступа в компьютерную сеть объединены в одном брелке. Для выхода из помещения необходимо предъявить РУТОКЕН RF, а при отключении идентификатора от USB-порта компьютера пользовательская сессия автоматически блокируется.

В РУТОКЕН RF используются пассивные радиочастотные метки стандартов EM-Marine, Indala, HID (рабочая частота 125 кГц). Это самые распространенные метки в России на сегодняшний день, считыватели, совместимые с ними, установлены в большинстве существующих систем контроля и управления доступом.

# 3.3.3 Подсистема защиты от вредоносного программного обеспечения

Согласно многочисленным исследованиям на сегодняшний день самой распространенной и наносящей самые большие убытки информационной угрозой являются вирусы, «троянские кони», утилиты-шпионы и прочее вредоносное программное обеспечение. Для защиты от него используются антивирусы. Причем этим средством обеспечения безопасности должен быть оборудован каждый компьютер вне зависимости от того, подключен он к Интернету или нет.

Для защиты информации в бухгалтерии ООО «Стиль» от вредоносного программного обеспечения будет использоваться Антивирус Касперского 2010.

Антивирус Касперского 2010 – это решение для базовой защиты компьютера от вредоносных программ. Продукт содержит основные инструменты для обеспечения безопасности ПК. Для полноценной защиты компьютера рекомендуется дополнительно использовать сетевой экран.

Признанные во всем мире антивирусные технологии защищают компьютер от таких современных информационных угроз, как:

* вирусы, троянские программы, черви, шпионские, рекламные программы и др.
* новые быстро распространяющиеся и неизвестные угрозы
* руткиты, буткиты и прочие изощренные угрозы
* ботнеты и другие незаконные способы скрытого удаленного управления компьютерами пользователей

В Антивирусе Касперского 2010 реализованы новейшие технологии защиты, позволяющие обеспечить безопасность и стабильную работу компьютера.

* Усовершенствованная Защита персональных данных, включающая модернизированную безопасную Виртуальную клавиатуру.
* Система мгновенного обнаружения угроз, моментально блокирующая новое вредоносное ПО
* Модуль Проверка ссылок, предупреждающий о зараженных или опасных веб-сайтах
* Проактивная защита нового поколения от неизвестных угроз
* Специальный Игровой профиль для временного отключения обновлений, проверки по расписанию и уведомлений.

Функции программы Антивирус Касперского 2010:

### Базовая защита:

* Защита от вирусов, троянских программ и червей
* Защита от шпионских и рекламных программ
* Проверка файлов в автоматическом режиме и по требованию
* Проверка почтовых сообщений (для любых почтовых клиентов)
* Проверка интернет-трафика (для любых интернет-браузеров)
* Защита интернет-пейджеров (ICQ, MSN)
* Проактивная защита от новых вредоносных программ
* Проверка Java- и Visual Basic-скриптов

### Предотвращение угроз:

* Поиск уязвимостей в ОС и установленном ПО
* Анализ и устранение уязвимостей в браузере Internet Explorer
* Блокирование ссылок на зараженные сайты
* Распознавание вирусов по способу их упаковки
* Глобальный мониторинг угроз (Kaspersky Security Network)

### Восстановление системы и данных:

* Возможность установки программы на зараженный компьютер
* Функция самозащиты программы от выключения или остановки
* Восстановление корректных настроек системы после удаления вредоносного ПО
* Наличие инструментов для создания диска аварийного восстановления

### Защита конфиденциальных данных:

* Блокирование ссылок на фишинговые сайты
* Защита от всех видов кейлоггеров

### Удобство использования:

* Автоматическая настройка программы в процессе установки
* Готовые решения (для типичных проблем)
* Наглядное отображение результатов работы программы
* Информативные диалоговые окна для принятия пользователем обоснованных решений
* Возможность выбора между простым (автоматическим) и интерактивным режимами работы
* Круглосуточная техническая поддержка
* Автоматическое обновление баз

# 3.3.4 Подсистема резервного копирования и архивирования

Один из эффективных методов борьбы с последствиями информационно-компьютерных катаклизм, модификации и потери информации – это правильная организация резервного копирования данных на предприятии.

Оптимальным решением для централизованного резервного копирования данных на рабочих станциях в корпоративной сети является Acronis True Image 9.1 Workstation — комплексный продукт для резервного копирования информации на рабочих станциях, входящих в состав локальной компьютерной сети предприятия. Эта программа позволяет создавать резервные копии:

1) жестких дисков и их разделов, со всеми хранящимися на них данными, операционными системами и приложениями;

2) наиболее важных для пользователя файлов и папок.

Поддержка как 64-разрядных, так и 32-разрядных версий ОС Windows обеспечивает эффективную защиту данных на компьютерах разных поколений. В случае фатальной ошибки программного или аппаратного обеспечения Acronis True Image 9.1 Workstation позволит выполнить полное восстановление системы или восстановление отдельных файлов и папок. Система может быть восстановлена как на прежний компьютер, так и на новый компьютер с другими аппаратными средствами или на виртуальную машину.

С консоли управления Acronis, входящей в состав Acronis True Image 9.1 Workstation, производится удаленное администрирование всех компьютеров в сети: установка агентов (приложений, необходимых для резервного копирования каждого компьютера), создание резервных копий и восстановление данных. Централизованное управление облегчает работу администратора и снижает общие затраты на обслуживание корпоративной сети.

Благодаря фирменной технологии Acronis Drive Snapshot Acronis True Image 9.1 Workstation производит резервное копирование данных без выключения и перезагрузки рабочих станций, что позволяет избежать перерывов в работе персонала.

# 3.3.5 Подсистема обнаружения сетевых атак

RealSecure Server Sensor - это программное решение, которое позволяет обнаруживать все атаки (т.е. на всех уровнях), направленные на конкретный узел сети. Помимо обнаружения атак RealSecure Server Sensor обладает возможностью проведения анализа защищенности и обнаружения уязвимостей на контролируемом узле.

Рис. 8. Компоненты RealSecure Server Sensor

RealSecure Server Sensor может и контролировать журналы регистрации ОС, а также журналы регистрации любых приложений, функционирующих под управлением этих ОС. Кроме того, RealSecure Server Sensor может обнаруживать атаки в сетях TCP/IP и SMB/NetBIOS, построенных на базе любых сетевых архитектур, поддерживаемых контролируемым компьютером.

# 3.3.6 Подсистема защиты информации в ЛВС

Подсистема защиты информации в ЛВС реализуется с помощью программного средства Secret Net. Система защиты информации Secret Net является программно-аппаратным комплексом, предназначенным для обеспечения информационной безопасности в локальной вычислительной сети.

Безопасность рабочих станций и серверов сети обеспечивается с помощью всевозможных механизмов защиты:

* усиленная идентификация и аутентификация,
* полномочное и избирательное разграничение доступа,
* замкнутая программная среда,
* криптографическая защита данных,
* другие механизмы защиты.

Администратору безопасности предоставляется единое средство управления всеми защитными механизмами, позволяющее централизованно управлять и контролировать исполнение требований политики безопасности.

Вся информация о событиях в информационной системе, имеющих отношение к безопасности, регистрируется в едином журнале регистрации. О попытках свершения пользователями неправомерных действий администратор безопасности узнает немедленно.

Существуют средства генерации отчетов, предварительной обработки журналов регистрации, оперативного управления удаленными рабочими станциями.

## Компоненты Secret Net:

Система Secret Net состоит из [трех компонент](http://www.avitek.ru/sn_comp.html):

* клиентская часть;
* сервер безопасности;
* подсистема управления.

Рис. 9. Компоненты системы Secret Net

Особенностью системы Secret Net является клиент-серверная архитектура, при которой серверная часть обеспечивает централизованное хранение и обработку данных системы защиты, а клиентская часть обеспечивает защиту ресурсов рабочей станции или сервера и хранение управляющей информации в собственной базе данных.

Сервер безопасности устанавливается на выделенный компьютер или контроллер домена и обеспечивает решение следующих задач:

* ведение центральной базы данных (ЦБД) системы защиты, функционирующую под управлением СУБД Oracle 8.0 Personal Edition и содержащую информацию, необходимую для работы системы защиты;
* сбор информации о происходящих событиях со всех клиентов Secret Net в единый журнал регистрации и передача обработанной информации подсистеме управления;
* взаимодействие с подсистемой управления и передача управляющих команд администратора на клиентскую часть системы защиты.

Подсистема управления Secret Net устанавливается на рабочем месте администратора безопасности и предоставляет ему следующие возможности:

* централизованное управление защитными механизмами клиентов Secret Net;
* контроль всех событий имеющих отношение к безопасности информационной системы;
* контроль действий сотрудников в ИС организации и оперативное реагирование на факты и попытки НСД;
* планирование запуска процедур копирования ЦБД и архивирования журналов регистрации.

Схема управления, реализованная в Secret Net, позволяет управлять информационной безопасностью в терминах реальной предметной области и в полной мере обеспечить жесткое разделение полномочий администратора сети и администратора безопасности.

# 3.3.7 Подсистема обеспечения целостности данных

Целостность информационной базы бухгалтерии обеспечивается встроенными механизмами программы 1С Бухгалтерия 7.7. При удалении помеченных объектов программа 1С Бухгалтерия 7.7 в автоматическом режиме осуществляет поиск ссылок на удаляемый объект. В диалоговом окне удаления помеченных объектов кнопка Удалить становится активной только после нажатия на кнопку Контроль и поиска ссылок на объект (рис. 10).

Рис. 10. Диалоговое окно удаления помеченных объектов программы 1С Бухгалтерия 7.7.

После осуществления контроля программой выдается сообщения о количестве объектов, которые нельзя удалить, так как их удаление вызовет нарушение ссылочной целостности и приведет к некорректной работе информационной базы (рис. 11).

Рис. 11. Сообщение о количестве неудаляемых объектов

В диалоговом окне удаления помеченных объектов появляется информация о ссылках на данный объект (рис. 12).

Рис. 12. Диалоговое окно удаления помеченных объектов программы 1С Бухгалтерия 7.7. после контроля целостности

В процессе работы системы 1С:Предприятие могут возникать различные внештатные ситуации - отключение питания компьютера «зависание» операционной системы, сбои оборудования и прочее. Такие ситуации, возникшие в процессе записи изменений в таблицы информационной базы системы 1С:Предприятие, могут привести к некорректному состоянию информационной базы. Внешние проявления некорректного состояния информационной базы могут быть различными, вплоть до невозможности запуска 1С:Предприятия.

Процедура «Тестирование и исправление информационных баз» предназначена для диагностики и устранения ошибочных состояний информационных баз, имеющих как формат DBF, так и формат MS SQL Server 6.5, при любом составе установленных компонент системы 1С:Предприятие.

# 3.3.8 Подсистема регистрации и учета

Данная подсистема также реализуется с помощью встроенных средств системы 1С Бухгалтерия 7.7. Регистрация и учет осуществляются с помощью специального режима Монитор.

Монитор пользователей является дополнительным средством, предназначенным для администрирования системы 1С:Предприятия.

Монитор позволяет просматривать список активных пользователей, то есть тех пользователей, которые в данный момент работают с информационной базой. Кроме того, монитор позволяет анализировать журнал регистрации действий, выполняемых пользователями за любые периоды времени (историю работы пользователей).

Для вызова основных функций Монитора пользователей в режиме запуска «Монитор» используются пункты «Активные пользователи» и «Журнал регистрации» колонки «Монитор» главного меню или соответствующие кнопки панели инструментов. Работа с этими функциями ведется также, как и в режиме запуска «1С:Предприятие».

## Архивирование журнала регистрации

Кроме основных функций (просмотра списка активных пользователей и журнала регистрации), в режиме запуска «Монитор» доступна функция архивирования журнала регистрации.

Режим просмотра журнала регистрации имеет возможность показывать события из текущего журнала, а также события тех периодов, которые помещены в архив. При этом, если выбранный для просмотра интервал включает периоды, за которые события помещены в архив, то извлечение данных из архива происходит автоматически. Разумеется, при обращении к данным архива на извлечение необходимой информации будет тратиться дополнительное время.

Для вызова функции архивирования журнала регистрации следует выбрать пункт меню «Архивирование журнала» из колонки «Монитор» главного меню или нажать соответствующую кнопку панели инструментов.

Режим архивирования может быть вызван только в том случае, если с данной информационной базой больше не работает ни один пользователь ни в каком режиме запуска 1С:Предприятия.

При вызове режима архивирования появляется диалог, в котором устанавливается период, за который данные журнала регистрации должны быть помещены в архив. В верхней части диалога выводится начальная и конечная даты текущего журнала.

Архивирование всегда выполняется, начиная с самых ранних событий текущего журнала: фактически, начальная граница архивируемого периода всегда определяется началом текущего журнала. В диалоге задается конечная граница периода архивирования.

# 3.4. Техническое задание на проектирование системы информационной безопасности

1.Общие сведения

1.1. Наименование системы

Система информационной безопасности ООО магазин «Стиль».

1.2. Шифр работ

Шифр работ − «ИБОООмС-3».

1.3. Заказчики и исполнители

1.3.1. Заказчик − ООО «Стиль», адрес: 644010, Россия, Омская область, г. Омск, ул. Ленинградская площадь 1.

1.3.2. Разработчик − Омский государственный технический университет, кафедра прикладной математики и информационных систем, адрес: Россия, 644050, г. Омск, пр. Мира, 11, тел. 65-20-48.

1.4. Основание для разработки

Договор № ### о создании Системы информационной безопасности ООО «Стиль». Утвержден 01.04.2010 г. директором ООО «Стиль» Узковой Л.А.

1.5. Сроки выполнения работ

1.5.1. Разработка и ввод «ИБОООмС-3» в действие реализуются в сроки: - начало работ – 01.04.2010 г.; - окончание работ– 31.05.2010 г.

1.6. Сведения об источниках финансирования работ

1.6.1. Источник финансирования – ООО «Стиль».

1.6.2. Порядок финансирования определяется договором № ###.

1.6.3. Объем финансирования – 80 000 рублей.

1.7. Порядок оформления и предъявления результатов работ

Результаты работ оформляются в порядке, установленном в договоре № ### от 01.04.10.

### 1.8. Порядок внесения изменений

### 1.8.1. В настоящее техническое задание (ТЗ) допускается внесение изменений и уточнение требований на основании решений заказчика. 1.8.2. Изменения к настоящему ТЗ должны оформляться дополнением или протоколом, подписанным заказчиком и исполнителем. Дополнение или протокол в этом случае будут являться неотъемлемой частью настоящего ТЗ.

2. Назначение и цели создания Системы

* 1. 2.1. Назначение системы

2.1.1. Разрабатываемая СИБ предназначена для комплексного решения задач обеспечения информационной безопасности в подразделении на основе новых технологий и оборудования, отвечающих современным требованиям, действующим нормативным документам, техническим требованиям и условиям органов государственного надзора. Основной функцией системы информационной безопасности является обеспечение адекватной защиты, целостности и конфиденциальности информационных ресурсов компании. Объект информационной защиты – ООО «Стиль».

2.2. Цели создания системы

Главной целью системы обеспечения информационной безопасности является обеспечение устойчивого функционирования предприятия, предотвращение угроз его безопасности, защита законных интересов предприятия от противоправных посягательств, недопущение хищения финансовых средств, разглашения, утраты, утечки, искажения и уничтожения служебной информации, обеспечение нормальной деятельности всех сотрудников предприятия. Еще одной целью системы информационной безопасности является повышение качества предоставляемых услуг и гарантий безопасности интересов клиентов.

3. Характеристики объекта защиты

ООО «Стиль» – это предприятие с распределенными по корпоративной сети коммерческими информационными ресурсами, подлежащими защите.

3.1. Объектом защиты является деятельность отдела бухгалтерии.

3.2. Управление должно вестись по технологическим этапам управленческого процесса: планирование, учет, контроль, анализ.

* 1. Сведения об условиях эксплуатации ИБОООмС-3

Условия эксплуатации должны соответствовать Гигиеническими требованиями к видеодисплейным терминалам, персональным электронно-вычислительным машинам и организации работы.

### 4. Требования к Системе в целом.

### 4.1. Требования к структуре и функционированию системы

### 4.1.1. Структураи составные части ИБОООмС-3

4.1.1.1. ИБОООмС-3 должна состоять:

- из CRM, разворачиваемой в отделе бухгалтерии;

- организационного обеспечения;

- нормативно-правового обеспечения;

- прикладного программного обеспечения (ППО);

- комплекса технических средств (КТС);

- информационного обеспечения (ИО).

4.1.1.3. ППО должно состоять из подсистем, соответствующих классу защищенности 2А.

4.1.2. Требования к способам и средствам защиты связи

для информационного обмена

4.1.2.1. На транспортном и сетевом уровнях взаимодействия (по семиуровневой модели OSI ГОСТ Р ИСО/МЭК 7498) должен использоваться стандартизованный стек протоколов TCP/IP.

4.1.2.2. Канальный и физический уровень взаимодействия должны реализовываться средствами локальных сетей пользователя и Интернет.

### 4.1.3. Требования к режимам функционирования ИБОООмС

Должно быть обеспечено функционирование СИБ Д в следующих режимах:

* штатный режим (режим работы, обеспечивающий выполнение пользователями своих функциональных обязанностей);
* сервисный режим (для проведения обслуживания, реконфигурации и пополнения новыми компонентами);
* аварийный режим.

4.2. Требования к численности и квалификации персонала системы и режиму его работы:

 Персонал ИБОООмС-3 должен состоять: - из пользователей ИБОООмС-3; - администратора ИБОООмС-3. 4.3. Требования к показателям назначения:

4.4. Требования к надежности:

4.4.1. Требования к надежности АИС УБП-2 устанавливаются для следующих составных частей системы:

- подсистем;

- КТС.

4.4.2. СИБ Д должна проектироваться как обслуживаемое восстанавливаемое изделие многократного применения (ГОСТ 27.003-90).

4.4.3. Оценка надежности системы должна проводиться с использованием основных показателей надежности (ГОСТ 24.701-86 и ГОСТ 27.003-90).

### 4.5. Требования безопасности

### 4.5.1. Программно-аппаратные средства ИБОООмС-3 должны обеспечивать безопасность обслуживающего персонала при эксплуатации, техническом обслуживании и ремонте с учетом требований ГОСТ 21552-84, ГОСТ 25861-83.

### 4.5.2. Электробезопасность должна соответствовать требованиям ГОСТ 12.1.030-81, ГОСТ 12.2.003, ГОСТ 12.2.007.0-75 и ГОСТ 12.2.007.13-2000.

### 4.5.3. Технические средства должны отвечать действующей системе Государственных стандартов безопасности труда и иметь сертификаты по электробезопасности и электромагнитной безопасности.

4.6. Требования к эргономике и технической эстетике: <отсутствуют>

4.7. Требования к эксплуатации, техническому обслуживанию, ремонту и хранению комплектов системы:

4.7.1. Эксплуатация ИБОООмС-3 должна производиться в соответствии с эксплуатационной документацией и Регламентом технического обслуживания.

4.7.2. Обслуживание ИБОООмС-3 должно производиться администратором информационной безопасности.

4.7.3. Допускается использование специализированных служб или подразделений на объектах внедрения для обслуживания и ремонта оборудования.

4.8. Требования к эксплуатации: <отсутствуют>

4.9. Требования к защите информации от несанкционированного доступа:

4.9.1. ИБОООмС-3 должны соответствовать требованиям класса 2А "Классификации автоматизированных систем и требования по защите информации" в соответствии с РД Гостехкомиссии.

4.9.2. Кроме технических мер должны применяться организационные меры защиты информации.

4.9.3. ИБОООмС-3 должна предоставлять средства аутентификации, авторизации, защиты целостности информации и защиты от атак.

### 4.10. Требования по сохранности информации при авариях

4.10.1. Должна быть обеспечена сохранность информации при авариях. 4.10.2. Должны быть предусмотрены средства для резервного копирования информации. В состав эксплуатационной документации должен входить регламент, определяющий процедуры резервного копирования, восстановления данных и программного обеспечения.

4.11. Требования к патентной чистоте: <отсутствуют>

4.12. Требования к стандартизации и унификации: <отсутствуют>

### 5. Требования к функциям

5.1. Подсистема управления доступом:

* должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов;
* должна осуществляться идентификация терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по их логическим адресам (номерам);
* должна осуществляться идентификация программ, томов, каталогов, файлов, записей, полей записей по именам;
* должно осуществляться управление потоками информации с помощью меток конфиденциальности. При этом уровень конфиденциальности накопителей должен быть не ниже уровня конфиденциальности записываемой на них информации.

**5.2. Подсистема регистрации и учета:**

Должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы). Регистрация выхода из системы или остановка не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:

* дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
* результат попытки входа: успешная или неуспешная (при НСД);
* идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;

Должна осуществляться регистрация выдачи печатных (графических) документов на "твердую" копию. Выдача должна сопровождаться автоматической маркировкой каждого листа (страницы) документа порядковым номером и учетными реквизитами АС с указанием на последнем листе документа общего количества листов (страниц). В параметрах регистрации указываются:

* дата и время выдачи (обращения к подсистеме вывода);
* спецификация устройства выдачи [логическое имя (номер) внешнего устройства], краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа;
* идентификатор субъекта доступа, запросившего документ;

Должна осуществляться регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов. В параметрах регистрации CRM должны указываться:

* дата и время запуска;
* имя (идентификатор) программы (процесса, задания);
* идентификатор субъекта доступа, запросившего программу (процесс, задание);
* результат запуска (успешный, неуспешный – несанкционированный);

Должна осуществляться регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации должны указываться:

* дата и время попытки доступа к защищаемому файлу с указанием ее результата: успешная, неуспешная – несанкционированная,
* идентификатор субъекта доступа;
* спецификация защищаемого файла.

Должна осуществляться регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: ПК, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей.

В параметрах регистрации должны указываться:

* дата и время попытки доступа к защищаемому объекту с указанием ее результата: успешная, неуспешная – несанкционированная;
* идентификатор субъекта доступа;
* спецификация защищаемого объекта [логическое имя (номер)];

Должен осуществляться автоматический учет создаваемых защищаемых файлов с помощью их дополнительной маркировки, используемой в подсистеме управления доступом. Маркировка должна отражать уровень конфиденциальности объекта;

Должно проводиться несколько видов учета (дублирующих) защищаемых носителей информации;

**5.3. Криптографическая подсистема:**

– должно осуществляться шифрование всей информации, записываемой на совместно используемые различными субъектами доступа (разделяемые) носители данных, в каналах связи, а также на съемные носители данных долговременной внешней памяти для хранения за пределами сеансов работы санкционированных субъектов доступа. При этом должны выполняться автоматическое освобождение и очистка областей внешней памяти, содержавших ранее незашифрованную информацию;

– доступ субъектов к операциям шифрования и криптографическим ключам должен дополнительно контролироваться подсистемой управления доступом.

5.4. **Подсистема обеспечения целостности:**

– должна быть обеспечена целостность программных средств СЗИ НСД, обрабатываемой информации, а также неизменность программной среды. При этом:

– целостность СЗИ НСД проверяется при загрузке системы по наличию имен (идентификаторов) компонент СЗИ;

– целостность программной среды обеспечивается отсутствием в АС средств разработки и отладки программ;

– должны осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания, где размещается АС, с помощью видеонаблюдения, использование строгого пропускного режима, специальное оборудование помещений АС;

 – должен быть предусмотрен администратор (служба) защиты информации, ответственный за ведение, нормальное функционирование и контроль работы СЗИ НСД;

 – должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест - программ, имитирующих попытки НСД;

– должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности;

– должны использоваться сертифицированные средства защиты.

### 6. Требования к видам обеспечения

### 6.1. Требования к информационному обеспечению: <отсутствуют>

6.2.Требования к математическому обеспечению: <отсутствуют>

6.3.Требования к информационному обеспечению: <отсутствуют>

6.4.Требования к лингвистическому обеспечению: <отсутствуют>

6.5. Требования к программному обеспечению

 6.5.1. Для построения СИБ необходимо использовать современные программные решения от ключевых вендоров в области информационной безопасности.

6.6. Требования к техническому обеспечению:

СИБ должна обеспечивать комплексную защиту приложений и всех объектов ИТ-инфраструктуры на базе передовых технологий безопасности, возможности работы с любыми аппаратными платформами (Windows, Unix/Linux), возможности масштабирования и гибкой конфигурации используемых аппаратно-программных средств безопасности.

6.7. Требования к метрологическому обеспечению: <отсутствуют>

6.8. Требования к организационному обеспечению:

Должна быть определена ответственность за нарушение режима безопасности информации.

7. Состав и содержание работ по созданию (развитию) системы.

7.1. Номер и наименование этапа:

1. проведение обследования: начало этапа – 01.04.2010 г., конец – 31.04.2010 г.
2. создание модели СИБ – начало этапа: 01.05.2010 г., конец – 31.05.2010 г.

8. Порядок контроля и приемки системы:

Контроль функционирования СИБ должен обеспечиваться:

* силами собственного подразделения по защите информации (администратора безопасности);

9. Требования к составу и содержанию работ по подготовке объекта автоматизации к вводу в действие: <отсутствуют>

10. Требования к документированию:

10.1. Документация, разрабатываемая в ходе создания ИБОООмС-3, должна соответствовать требованиям ГОСТ 34.201-89.

10.2. Проектная документация на систему защиты информации должна включать следующие документы по информационной безопасности:

* руководство пользователя;
* руководство администратора СЗИ;
* тестовая и инструктивно-методическая документация;
* конструкторская (проектная) документация.

11. Источники разработки:

* 1. Техническое задание на создание автоматизированной системы. ГОСТ 34.602-89.
	2. Виды, комплектность и обозначение документов при создании автоматизированных систем. ГОСТ 34.201-89.
	3. Требования к содержанию документов. РД 50-34.698-90.

# Заключение

В современном мире информационный ресурс стал одним из наиболее мощных рычагов экономического развития. Владение информацией необходимого качества в нужное время и в нужном месте является залогом успеха в любом виде хозяйственной деятельности. Монопольное обладание определенной информацией оказывается зачастую решающим преимуществом в конкурентной борьбе и предопределяет, тем самым, высокую цену информационного фактора. Широкое внедрение персональных компьютеров вывело уровень информатизации деловой жизни на качественно новую ступень. Ныне трудно представить себе фирму или предприятие (включая самые мелкие), которые не были бы вооружены современными средствами обработки и передачи информации. В ПК на носителях данных накапливаются значительные объемы информации, представляющей большую ценность для ее владельца.

Однако создание индустрии переработки информации, давая объективные предпосылки для грандиозного повышения эффективности жизнедеятельности человечества, порождает целый ряд сложных и крупномасштабных проблем. Одной из таких проблем является надежное обеспечение сохранности и установленного статуса использования информации, циркулирующей и обрабатываемой в распределенных информационных системах.

В рамках данной курсовой работы спроектирована система информационной безопасности для бухгалтерии ООО магазин «Стиль».

В ходе выполнения курсовой работы были решены следующие задачи:

1. Обследована инфраструктура ООО магазин «Стиль» и определены исходные данные для проектирования системы ИБ;
2. Разработана концепция ИБ;
3. Разработана система информационной безопасности.

# Библиографический список

* 1. Силаенков А.Н. Проектирование системы информационной безопасности: учеб. пособие – Омск: Изд-во ОмГТУ, 2009. – 128 с.
	2. **Руководящий документ Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации от 30 марта 1992 г.**
	3. Грязнов Е.С., Панасенко С.А. Безопасность локальных сетей. – М.: Вузовский учебник, 2006.- 525 с.
	4. Козлачков П.С. Основные направления развития систем информационной безопасности. – М.: финансы и статистика, 2004.- 736 с.
	5. Леваков Г.Н. Анатомия информационной безопасности. – М.: ТК Велби, издательство Проспект, 2004.- 256 с.
	6. Соколов Д.Н., Степанюк А.Д. Защита от компьютерного терроризма. – М.: БХВ-Петербург, Арлит, 2002.- 456 с.
	7. Сыч О.С. Комплексная антивирусная защита локальной сети. – М.: финансы и статистика, 2006.- 736 с.
	8. [Швецова Н.Д. Системы технической безопасности: актуальные реалии.](http://www.security.strongdisk.ru/i/146/) – Спб: Питер, 2004. – 340 с.
	9. http://www.lghost.ru/lib/security/kurs5/theme01\_chapter04.htm
	10. http://www.globaltrust.ru/
	11. http://www.arnis.ru/gost\_17799\_common.htm