Введение

Целью данного дипломного проекта является аудит информационной безопасности для предприятия ОАО «РОСТСТРОЙ». Необходимо пояснить, что подразумевается под понятием «аудит».

Аудит информационной безопасности – системный процесс получения объективных качественных и количественных оценок о текущем состоянии информационной безопасности компании (организации, предприятия) в соответствии с определенными критериями и показателями безопасности.

Актуальность проведенной работы обусловлена тем, что обеспечение безопасности информации – процесс непрерывный, то есть в условиях постоянно изменяющейся обстановки в сфере информационных технологий, в условиях появления все новых угроз конфиденциальности информации, а также и новых технических и программных средств, служащих для реализации этих угроз, необходим постоянный контроль надежности системы защиты. Именно эту функцию и выполняет аудит информационной безопасности. В связи с этим возникают вопросы о методах и результатах проведения аудита, ответы на которые и представлены в данном проекте. При этом речь в данном случае идет не о постоянном внутреннем аудите, который должна вести каждая организация, старающаяся наладить свою информационную безопасность, а о внешнем аудите, проводимом сторонней организацией, отличающимся своей независимостью и комплексностью.

Объектом исследования, проведенного в рамках дипломного проекта, стала система защиты информации предприятия ОАО «РОСТСТРОЙ», а его задачей – выявление ее недостатков и возможностей реализации угроз конфиденциальной информации. Упор был сделан на изучение функционирования информационной системы организации.

Целью исследования, а также и дипломного проекта, стала разработка комплекса мер (рекомендаций) по улучшению системы защиты информации организации на основе выделенных типов угроз и определение приоритетных направлений ее развития на основе анализа надежности полученной системы защиты.

Практическая значимость дипломного проекта заключается в реализации разработанного комплекса мер по защите информации в деятельности ОАО «РОСТСТРОЙ», а также в дальнейшем развитии системы защиты информации по выделенным в ходе работы направлениям, что позволит существенно снизить информационные риски в будущем.

1 Описание предприятия

1.1 Общие сведения о предприятии ОАО «РОСТСТРОЙ»

Открытое акционерное общество «РОСТСТРОЙ» образовано в 1993г. ОАО «РОСТСТРОЙ» является предприятием стройиндустрии, осуществляющим свою деятельность на строительном рынке по принципу холдинга. В структуру предприятия входят несколько собственных подразделений, каждое из которых выполняет определенный круг задач, что позволяет осуществлять полный цикл услуг, от производства строительных материалов и строительства, до транспортных услуг.

За период своей многолетней истории, предприятие специализировалось не только на выполнении ремонтно-строительных работ, обслуживании и ремонте оборудования, но также и на производстве столярных и металлических изделий. Развиваясь и меняясь вместе с рынком строительных услуг, неизменным остается высокое качество выполняемых работ. Сейчас ОАО «РОСТСТРОЙ» имеет возможность выполнять работы по строительству, ремонту и реконструкции объектов гражданского строительства, жилищно-коммунального хозяйства, а также энергетического и металлургического комплексов.

В ОАО «РОСТСТРОЙ» работает команда высококвалифицированных специалистов с огромным опытом работы. Здесь имеется свой штат строителей, монтажников металлоконструкций, теплоизолировщиков, футеровщиков, промышленных альпинистов, кровельщиков, газо- и электросварщиков, поэтому данное предприятие можем качественно реализовывать проекты любой сложности в кратчайшие сроки. Наличие собственной производственной базы позволяет успешно выполнять любые поставленные заказчиком задачи.

1.2 Основные направления деятельности ОАО «РОСТСТРОЙ»

Предприятие ОАО «РОСТСТРОЙ» обеспечивает:

1. Производство ЖБИ, бетона, бетонного раствора

 Производство бетонных, железобетонных изделий, металлоконструкций любой сложности, опалубки, товарного бетона, строительного раствора. За период существования производства освоен практически весь комплекс типовых железобетонных, бетонных изделий гражданского жилищного строительства (плиты, перекрытия шириной 1,2 и 1,5м, дорожные плиты, плиты фундаментов, лестничные марши, площадки, перемычки всех типов, телефонные колодцы, промзабор, прогоны, сваи до 12м, ж/б колодцы и др.). Продукция завода поставляется на объекты гражданского, жилищного строительства, на строительство уникальных сооружений культурно - социального назначения.

1. Производство и монтаж элементов фасада: оконные системы (окна из ПВХ и алюминиевого профиля), воротные системы проектирование, изготовление, монтаж светопрозрачных конструкций любой сложности из алюминиевого и ПВХ-профиля (окна, двери, витражи, фасады зданий, крышные конструкции, фонари, зимние сады, остекление балконов и лоджий, в том числе раздвижных, офисные перегородки); ворота всех типов: подъемно-поворотные, секционные, распашные, сдвижные, кованные, роллеты.
2. Производство тротуарной плитки: предприятие производит тротуарную плитку различных типоразмеров. Широкий ассортимент производимой плитки (а также формы, цветовые решения, элементы фактуры и декора) и высокое качество и надежность в эксплуатации, отвечают современным требованиям любого объекта строительства.
3. Строительство: подрядная деятельность, производство строительно-монтажных работ, ремонтно-восстановительных работ, строительная реконструкция. ОАО «РОСТСТРОЙ» выполняет общестроительные работы, реконструкцию промышленных комплексов, зданий, сооружений, объектов жилья, социально-бытового назначения по всему спектру строительных работ.
4. Транспорт: наряду с производством строительных материалов и строительной деятельностью данное предприятие организует поставки жби (строительных материалов) и бетонных растворов на любые объекты строительства на территории Ростовской области. Предприятие имеет в своем распоряжении собственный специализированный автомобильный парк, оснащенный в соответствии с современными требованиями, это позволяет осуществлять полный комплекс автотранспортных услуг. Отличительные особенности: мобильность и оперативность.

1.3 Структура предприятия ОАО «РОСТСТРОЙ»

Организационная структура предприятия – совокупность управленческих звеньев находящихся в строгой соподчиненности взаимосвязанных и взаимодействующих между собой. Организационная структура предприятия определяет область ответственности и функциональную значимость каждого элемента входящего в состав данной структуры.

В структуре строительного предприятия ОАО «РОСТСТРОЙ» есть все отделы и службы, каждый из которых четко выполняет свою функцию, при полном взаимодействии со всеми подразделениями предприятия. И, конечно же, квалифицированные специалисты, руками которых выполняются работы. Такая структура предприятия позволяет успешно и качественно выполнять работы одновременно на нескольких объектах.

Структура строительного предприятия располагает всеми специалистами для производства общестроительных и специализированных работ.

Фирма имеет сильный инженерно-технический персонал, который способен решать сложнейшие производственные, технологические и конструкторские задачи.

В распоряжении фирмы также имеется проектный отдел. Технические решения проекта разрабатываются исходя из технологий, прогрессивных показателей расхода основных материалов и трудоемкости строительства.

 1.4 Структура сети предприятия ОАО «РОСТСТРОЙ»

Рис.1 Структура предприятия ОАО «РОСТСТРОЙ»

Рисунок 1 - Структура предприятия ОАО «РОСТСТРОЙ»

Отдел материально-технического снабжения

Зам. директора по экономическим вопросам

Отдел безопасности

Секретарь

Отдел кадров

Главный бухгалтер

Юридический отдел

Транспортный отдел

Отдел тротуарной плитки

Отделочный отдел

Монтажный отдел

Отдел ЖБИ

Отдел охраны труда и техники безопасности

Строительный отдел

Производственный отдел

Зам. директора по производственным вопросам

Технологический отдел

Проектный отдел

Главный инженер

Директор

 1.5 Информационные потоки предприятия ОАО «РОСТСТРОЙ»

Рисунок 2 - Структура сети с подключением устройств защиты предприятия

ОАО «РОСТСТРОЙ»

Информационными потоками – называется строго определенная последовательность циклов передвижения информации на предприятии.

В основном деятельность сотрудников в сети сводится к работе с базами данных, использованием информации хранящейся на Web-сервере, работа с Интернет протоколами. В связи с этим можно дать следующую классификацию информационных потоков:

* Пакеты больших размеров -  (Web Server)
* Пакеты средних размеров -  (Data Base)
* Пакеты малых размеров -  (POP mail, SMTP mail)

 2 Аудит информационной безопасности и необходимость его проведения

Рисунок 3 - Информационные потоки предприятия ОАО «РОСТСТРОЙ»

В настоящее время информация является одним из самых ценных ресурсов в любой компании (организации, предприятии), а для некоторых - и основным производственным ресурсом, ведь от сохранности информации и бесперебойного доступа к ней нередко зависят важные технологические и бизнес-процессы. Но с развитием информационных технологий также стремительно возрастает риск утечки информации, внешнего вмешательства в работу информационно-телекоммуникационной системы (ИТС), заражение вирусами. Важно осознавать реальное состояние защищенности ценных ресурсов ИТС, чтобы противостоять внешним и внутренним угрозам ее безопасности. В этом реальную помощь может оказать независимое исследование состояния безопасности ИТС – аудит безопасности.

Аудит информационной безопасности - это системный процесс получения объективных качественных и количественных оценок текущего состояния корпоративной ИТС в соответствии с критериями информационной безопасности.

Для того чтобы оценить реальное состояние защищенности ресурсов ИТС и ее способность противостоять внешним и внутренним угрозам безопасности, необходимо регулярно проводить аудит информационной безопасности.

Аудит информационной безопасности можно разделить на два вида:

- экспертный аудит информационной безопасности, в ходе которого выявляются недостатки в системе мер защиты информации на основе опыта экспертов, участвующих в процедуре аудита;

 - аудит информационной безопасности на соответствие международному стандарту ISO/IEC 27001:2005 «Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования», разработанному Международной организацией по стандартизации (ISO) и Международной электротехнической комиссией (IEC) на основе британского стандарта BS 7799-2:2002 «Системы управления информационной безопасностью. Спецификация и руководство по применению».

В число задач, которые решаются в ходе проведения аудита информационной безопасности входят:

 - сбор и анализ исходных данных об организационной и функциональной структуре ИТС организации, необходимых для оценки состояния информационной безопасности;

- анализ существующей политики обеспечения информационной безопасности на предмет полноты и эффективности;

- анализ информационных и технологических рисков связанных с осуществлением угроз информационной безопасности;

- осуществление тестовых попыток несанкционированного доступа к критически важным узлам ИТС и определение уязвимости в установках защиты данных узлов;

- формирование рекомендаций по разработке (или доработке) политики обеспечения информационной безопасности на основании анализа существующего режима информационной безопасности;

- формирование предложений по использованию существующих и установке дополнительных средств защиты информации для повышения уровня надежности и безопасности ИТС организации.

Цель проведения экспертного аудита информационной безопасности - оценка состояния безопасности ИТС и разработка рекомендаций по применению комплекса организационных мер и программно-технических средств, направленных на обеспечение защиты информационных и других ресурсов ИТС от угроз информационной безопасности.

Экспертный аудит информационной безопасности является начальным этапом работ по созданию комплексной системы защиты информации ИТС. Эта подсистема представляет собой совокупность мер организационного и программно-технического уровня, которые направлены на защиту информационных ресурсов ИТС от угроз информационной безопасности, связанных с нарушением доступности, целостности и конфиденциальности хранимой и обрабатываемой информации.

Экспертный аудит информационной безопасности позволяет принять обоснованные решения по использованию мер защиты, необходимых для отдельно взятой организации, оптимальных в соотношении их стоимости и возможности осуществления угроз нарушения информационной безопасности.

Аудит информационной безопасности на соответствие международному стандарту ISO/IEC 27001:2005 представляет собой перечень требований к системе менеджмента информационной безопасности (СМИБ), обязательных для сертификации. Стандарт устанавливает требования к разработке, внедрению, функционированию, мониторингу, анализу, поддержке и совершенствованию документированной СМИБ в контексте существующих бизнес-рисков организации.

Таким образом, результатом проведенного аудита на соответствие международному стандарту ISO/IEC 27001:2005 является:

- описание области деятельности СМИБ;

- методику определения существенных активов;

- список (опись, реестр) существенных активов организации и их ценность (критичность);

- методику оценки рисков;

- отчет по оценке рисков;

- критерии для принятия рисков;

- заявление о принятии (одобрении) остаточных рисков;

- план обработки рисков;

- список политик, руководств, процедур, инструкций, необходимых для функционирования СМИБ организации. Рекомендации по их разработке.

2.1 Шаги проведения комплексного аудита безопасности ИС

* Информационное обследование ИС.
* Анализ соответствия предъявляемым требованиям.
* Инструментальное исследование элементов инфраструктуры компьютерной сети и корпоративной информационной системы.
* Анализ уязвимостей и оценка рисков.
* Рекомендации по результатам организационно-технического анализа системы ИБ предприятия.

По желанию Заказчика может быть проведен аудит по отдельным видам работ, по отдельным объектам ИС (ЛВС, периметр защиты ИС, автоматизированные системы) либо выполнены дополнительные работы:

* Анализ документооборота предприятия категории "коммерческая тайна" на соответствие требованиям нормативных документов отраслевого, федерального уровня и внутренним требованиям предприятия по обеспечению.
* Предпроектное обследование объектов информатизации.
* Тесты на проникновение.

3 Анализ системы безопасности предприятия ОАО «РОСТСТРОЙ»

## 3.1 Анализ существующей системы инженерно-технической защиты информации. Перечень разработанных рекомендаций по повышению эффективности системы инженерно-технической защиты информации

На предприятии осуществлено ограждение территории заборами, усовершенствованными с помощью нескольких валиков скрученной колючей проволоки, регулярно осуществляется обход территории завода охранниками, средства видеонаблюдения отсутствуют, используется система дежурного и аварийного охранного освещения.

На предприятии используется подсистема контроля и управления доступом.

Подсистема контроля и управления доступом (СКУД) представляет собой совокупность организационных мер, оборудования и приборов, инженерно-технических сооружений, алгоритмов и программ, которая автоматически выполняет в определенных точках объекта в заданные моменты времени, следующие основные задачи:

- разрешает проход уполномоченным субъектам (сотрудникам, посетителям, транспорту);

- запрещает проход всем остальным.

Объект разбит на зоны доступа, в каждую из которых имеет право проходить строго определенные лица (субъекты). Для доступа в зоны субъекту необходимо пройти набор точек доступа. В каждой точке доступа установлены считыватели и преграждающие устройства.

На предприятии имеются две проходные, оборудованные двустворчатыми воротами с шириной проезда 6 метров. Через одну из них осуществляется проход персонала и проезд на личном автотранспорте к зданию администрации. Доступ на территорию предприятия осуществляется посредством смарт-карт. Смарт-карта представляет собой пластиковую карточку, по размерам соответствующую обычной кредитной карточке, в которую заключены микропроцессор и запоминающее устройство.

Внутренняя архитектура смарт-карты включает микропроцессор, позволяющий использовать сложные способы кодирования информации, постоянную память, в которую зашиты команды для процессора, оперативную память, используемую в качестве рабочей, и перезаписываемую память для чтения и записи информации извне.

Для контроля над деятельностью персонала на контрольно-пропускном пункте установлена система контроля доступа, состоящая из считывателя карт, контроллера обработки информации от считывателя, а также программного обеспечения (с персональным компьютером) для ведения непрерывного протокола событий обо всех действиях персонала.

К системе контроля доступа подключены шлагбаум, и турникеты что позволяет открывать шлагбаум автоматически при поднесении карточки к считывателю.

На входе установлены два турникета и четыре считывателя – на вход и на выход. Для прохода через турникет сотруднику необходимо поднести карточку к соответствующему считывателю. Все считыватели подключены к контроллерам системы контроля доступа, которые принимают решение о допуске сотрудников, а также ведут непрерывный протокол всех событий.

Вторая проходная предназначена для грузового транспорта. В непосредственной близости от проходной расположена стоянка грузовых автомобилей, где и осуществляется погрузка-разгрузка материалов.

Доступ на территорию предприятия через вторую проходную осуществляется с помощью системы пропусков. Пропуск выписывается заранее. Государственные номера автотранспорта, цель прибытия, время погрузки и разгрузки фиксируются в специальном журнале.

В здании администрации организована система охранной сигнализации: на окна и входные двери установлены специальные устройства, передающие сигнал тревоги при открывании, во многих помещениях установлены датчики движения.

Разработанные рекомендации:

1. Организовать на предприятии охранное телевидение.

2. Оборудовать входные двери специальными замками, позволяющими регулировать доступ в помещения.

3. Заменить и установить армированную колючую ленту на определенных участках периметра.

4. Установить противотаранное устройство на проходной для автотранспорта.

5. Заменить двустворчатые ворота на проходной для автотранспорта.

6. Установить устройство защиты телефонных линий в кабинете директора (Цикада М, Зевс, Генератор Соната АВ 1М).

7. Установить прибор для защиты помещений от прослушивания через акустический и вибрационный каналы в помещении, предназначенном для конфиденциальных переговоров (Зевс, Генератор ВГШ-103, виброакустический генератор SI-3001, шумогенератор PNG-200).

8. Использовать технические средства для повышения отказоустойчивости и защиты оборудования от сбоя электропитания (источники бесперебойного питания APC Smart 420 VA и источник бесперебойного питания IPPON PowerPro Back 400 VA).

9. Использовать программно-аппаратные средства криптографической защиты линии конференцсвязи директора (аппаратно-программный комплекс шифрования (АПКШ) "Континент", аппаратно-программный криптографический комплекс «Верба» и «ШИП», аппаратно-программный комплекс ViPNet).

## 3.2 Анализ существующей системы документооборота. Перечень разработанных рекомендаций.

Документы, содержащие конфиденциальную информацию, обрабатываются в следующих отделах: бухгалтерия, отдел кадров, юридический одел, отдел безопасности. К ним относятся:

- бухгалтерский баланс;

- отчеты о прибылях и убытках в приложениях к балансу и налоговым декларациям;

- первичные документы (декларация по налогу на добавленную стоимость, платежные поручения, кассовые ордера, выписки банка, справки о состоянии расчетного счета, банковские гарантии и т.д.)

- сводные учетные документы;

- сведения бухгалтерских регистров;

- внутренняя отчетность;

- данные налогового и управленческого учета;

- плановые и фактические показатели финансово-хозяйственной деятельности;

- сведения о личных доходах каждого работника;

- сведения о долговых обязательствах предприятия, в том числе о размерах и условиях полученных кредитов и займов;

- механизм ценообразования (прямые издержки, накладные расходы, норма прибыли);

- результаты изучения рынка, оценка состояния и перспектив развития рыночной конъюнктуры;

- сведения о рыночной стратегии фирмы и об оригинальных методах продвижения товаров;

- проекты прайс-листов и условия предоставления скидок;

- сведения о предполагаемых закупках, о полученных заказах и об объемах взаимных поставок по долгосрочным договорам;

- сведения о предприятии как о торговом партнере;

- данные обо всех контрагентах, деловых партнерах и конкурентах предприятия, которые не содержатся в открытых источниках;

- торговые соглашения, которые по договоренности сторон считаются конфиденциальными;

- сведения о проведении, повестках дня и результатах служебных совещаний;

- сведения о подготовке и результатах переговоров с деловыми партнерами предприятия;

- состояние программного и компьютерного обеспечения фирмы;

- сведения о структуре производства, производственных мощностях, типах и размещении оборудования, запасах сырья, материалов, комплектующих изделий и готовой продукции;

- направления и объемы инвестиций;

- плановые экономические показатели;

- планы расширения или свертывания производства различных видов продукции и их технико-экономические обоснования;

- сведения о новых материалах и технологии их применения, о комплектующих изделиях, которые придают продукции новые качества;

- сведения о модернизации известных технологий, которая позволяет повысить конкурентоспособность продукции;

- сведения о целях, задачах и программах перспективных исследований;

- конструкционные характеристики создаваемых изделий и параметры разрабатываемых технологических процессов (габариты, компоненты, режимы обработки и т. п.);

- особенности конструкторско-технологических решений и дизайнерского оформления, которые могут изменить рентабельность изделий;

- условия экспериментов и характеристика оборудования, на котором они проводились.

При ознакомлении посторонних лиц с данными документами возможны следующие последствия:

- разрыв (или ухудшение) деловых отношений с партнерами;

- срыв переговоров, потеря выгодных контрактов;

- невыполнение договорных обязательств;

- необходимость проведения дополнительных рыночных исследований;

- отказ от решений, ставших неэффективными из-за огласки информации, и, как следствие, финансовые потери, связанные с новыми разработками;

- ущерб авторитету или деловой репутации фирмы;

- более жесткие условия получения кредитов;

- трудности в снабжении и приобретении оборудования и т. д.

Система документооборота на предприятии заключается в следующем.

На предприятии различают три основных потока документации:

- входящие документы, поступающие из других организаций;

- исходящие документы, отправляемые в другие организации;

- внутренние документы, создаваемые на предприятии и используемые работниками предприятия в управленческом процессе.

Все документы, поступающие на предприятие, проходят первичную обработку, предварительное рассмотрение, регистрацию, рассмотрение руководством, передачу на исполнение.

Не вскрываются и передаются по назначению документы с пометкой “лично”.

Предварительное рассмотрение документов проводится секретарем с целью распределения поступивших документов на:

- направляемые на рассмотрение руководителю предприятия;

- направляемые непосредственно в структурные подразделения или конкретным исполнителям.

Без рассмотрения руководителем передаются по назначению документы, содержащие текущую оперативную информацию или адресованные в конкретные подразделения. Это позволяет освободить руководителя предприятия от рассмотрения мелких текущих вопросов, решение по которым могут принимать ответственные исполнители.

На рассмотрение руководства передаются документы, адресованные руководителю предприятия и документы, содержащие информацию по наиболее важным вопросам деятельности предприятия.

Если документ должен исполняться несколькими подразделениями или должностными лицами, его размножают в нужном количестве экземпляров.

Документы, подлежащие отправке в другую организацию, сортируют, упаковывают, оформляют как почтовое отправление и сдают в отделение связи.

Внутренние документы предприятия передаются исполнителям под расписку в регистрационной форме.

Регистрации подлежат все документы, требующие специального учета, исполнения и использования в справочных целях независимо от способа получения. Сам процесс регистрации - это снятие с документа показателей (реквизитов) и занесение их в определённую регистрационную форму (журнал, ПЭВМ) для создания базы данных о документах учреждения.

Каждый документ, отнесённый к числу регистрируемых, получает свой регистрационный номер.

Документы регистрируются один раз. Регистрация внутренних документов проводится, децентрализовано по группам внутри отделов.

Для входящих, исходящих и внутренних документов ведутся раздельные регистрационные формы с самостоятельными регистрационными номерами.

К документам, содержащим конфиденциальную информацию, имеют доступ начальники отделов и их заместители. Все документы хранятся в столах у начальников отделов, передаются в другие структурные подразделения лично начальником отдела или его заместителем. Учет документов, содержащих конфиденциальную информацию, ведется вместе с учетом остальных документов. Доступ к документам в электронном виде разграничен системой доступа к файлам.

Недостатками данной системы документооборота является то, что невозможно отследить четкие маршруты прохождения документов и распределить поступающие документы по степени конфиденциальности. Конфиденциальный документ, проходя согласование, визирование у многих руководителей и во многих подразделениях, оказывается в руках большого числа посторонних людей - секретарей, заместителей, помощников руководителей, не имеющих к нему прямого отношения. Также человек, получивший доступ в кабинет начальника отдела, практически беспрепятственно может ознакомиться с конфиденциальными документами, хранящимися в столе.

Необходим комплекс административных, процедурных и программно - аппаратных мер, направленных на минимизацию утечки информации через сотрудников: сократить количество людей, допущенных к конкретной информации, до минимально необходимого, жестко разграничивать доступ к хранилищам информации, контролировать, кто получил информацию, защищать процесс ее передачи.

# Разработанные рекомендации:

1. Создать на предприятии сектор по работе с документами, содержащими конфиденциальную информацию.

2. Разработать «Инструкцию по обеспечению сохранности коммерческих тайн на предприятии» (Приложение А).

3.3Анализ существующей системы компьютерной безопасности. Перечень разработанных рекомендаций по повышению компьютерной безопасности

На предприятии существует локальная вычислительная сеть (ЛВС). ЛВС управляется операционной системой Windows 2000 Server.

В качестве основного средства бухгалтерского учета на предприятии используется сетевая версия программы 1С, прекрасно зарекомендовавшая себя по всем характеристикам. Программа поддерживается операционной системой Windows 98/2000/NT/ХР и сервисно обслуживается специально подготовленным для этого персоналом фирмы-продавца.

Так как ОАО «РОСТСТРОЙ» имеет вертикальную структуру и точно известно, какой сотрудник и к какой информации должен иметь доступ, то на предприятии используется вариант сети с выделенным сервером. Только в такой сети существует возможность администрирования прав доступа. Топология типа «звезда» представляет собой более производительную структуру, каждый компьютер, в том числе и сервер, соединяется отдельным сегментом кабеля с центральным концентратором (HAB). Основным преимуществом такой сети является её устойчивость к сбоям, возникающим вследствие неполадок на отдельных ПК или из-за повреждения сетевого кабеля.

Сервер установлен в специальном помещении (серверной), которое удовлетворяет требованиям, то есть уровень шума в помещении минимален, помещение изолированно от других, следовательно, доступ к серверу ограничен. В то же время более удобно проводить обслуживание сервера.

Вся кабельная сеть проложена в пустоте между фальш-полом и плитами перекрытия этажей.

Компьютеры предприятия сгруппированы в рабочие группы, что дает два важных преимущества сетевым администраторам и пользователям. Наиболее важное - серверы домена составляют единый административный блок, совместно использующий службу безопасности и информацию учетных карточек пользователя. Каждая рабочая группа имеет одну базу данных, содержащую учетные карточки пользователя и групп, а также установочные параметры политики безопасности. Все серверы домена функционируют либо как первичный контроллер домена, либо как резервный контроллер домена, содержащий копию этой базы данных. Это означает, что администраторам нужно управлять только одной учетной карточкой для каждого пользователя, и каждый пользователь должен использовать и помнить пароль только одной учетной карточки.

Windows 2000 Server имеет средства обеспечения безопасности, встроенные в операционную систему. Ниже рассмотрены наиболее значимые из них:

1 Слежение за деятельностью сети.

Windows 2000 Server дает много инструментальных средств для слежения за сетевой деятельностью и использованием сети. ОС позволяет просмотреть сервер и увидеть, какие ресурсы он использует увидеть пользователей, подключенных к настоящему времени к серверу и увидеть, какие файлы у них открыты; проверить данные в журнале безопасности; записи в журнале событий; и указать, о каких ошибках администратор должен быть предупрежден, если они произойдут.

2 Начало сеанса на рабочей станции.

Всякий раз, когда пользователь начинает сеанс на рабочей станции, экран начала сеанса запрашивает имя пользователя, пароль и домен. Затем рабочая станция посылает имя пользователя и пароль в домен для идентификации. Сервер в домене проверяет имя пользователя и пароль в базе данных учетных карточек пользователей домена. Если имя пользователя и пароль идентичны данным в учетной карточке, сервер уведомляет рабочую станцию о начале сеанса. Сервер также загружает другую информацию при начале сеанса пользователя, как, например, установки пользователя, свой каталог и переменные среды.

По умолчанию не все учетные карточки в домене позволяют входить в систему. Только карточкам групп администраторов, операторов сервера, операторов управления печатью, операторов управления учетными карточками и операторов управления резервным копированием разрешено это делать.

Для всех пользователей сети предприятия предусмотрено свое имя и пароль.

3 Учетные карточки пользователей.

Каждый клиент, который использует сеть, имеет учетную карточку пользователя в домене сети. Учетная карточка пользователя содержит информацию о пользователе, включающую имя, пароль и ограничения по использованию сети, налагаемые на него. Имеется возможность также сгруппировать пользователей, которые имеют аналогичные ресурсы, в группы; группы облегчают предоставление прав и разрешений на ресурсы, достаточно сделать только одно действие, дающее права или разрешения всей группе. Таблица 1 показывает содержимое учетной карточки пользователя.

Таблица 1 - Содержимое учетной карточки

|  |  |  |
| --- | --- | --- |
| Учетная карточка пользователя | Элемент учетной карточки | Комментарии |
| Username | Имя пользователя | Уникальное имя пользователя, выбирается при регистрации.  |
| Password | Пароль | Пароль пользователя. |
| Full name | Полное имя | Полное имя пользователя. |
| Logon hours | Часы начала сеанса | Часы, в течение которых пользователю позволяется входить в систему. Они влияют на вход в систему сети и доступ к серверу. Так или иначе, пользователь вынужден будет выйти из системы, когда его часы сеанса, определенные политикой безопасности, истекут. |
| Logon workstations | Рабочие станции | Имена рабочих станций, на которых пользователю позволяется работать. По умолчанию пользователь может использовать любую рабочую станцию, но возможно введение ограничений. |
| Expiration date | Дата истечения срока | Дата в будущем, когда учетную карточку автоматически исключают из базы, полезна при принятии на работу временных служащих. |
| Home directory | Собственный каталог | Каталог на сервере, который принадлежит пользователю; пользователь управляет доступом к этому каталогу. |
| Logon script | Сценарий начала сеанса | Пакетный или исполняемый файл, который запускается автоматически, когда пользователя начинает сеанс. |
| Profile | Установки (параметры) | Файл, содержащий запись о параметрах среды рабочего стола пользователя, о таких, например, как сетевые соединения, цвета экрана и установочные параметры, определяющие, какие аспекты среды, пользователь может изменить. |
| Account type | Тип учетной карточки | Тип учетной карточки – глобальный или локальный. |

4 Журнал событий безопасности.

Windows 2000 Server позволяет определить, что войдет в ревизию и будет записано в журнал событий безопасности всякий раз, когда выполняются определенные действия или осуществляется доступ к файлам. Элемент ревизии показывает выполненное действие, пользователя, который выполнил его, а также дату и время действия. Это позволяет контролировать как успешные, так и неудачные попытки каких-либо действий.

Журнал событий безопасности для условий предприятия является обязательным, так как в случае попытки взлома сети можно будет отследить источник.

Таблица включает категории событий, которые могут быть выбраны для ревизии, а также события, покрываемые каждой категорией.

Таблица 2 - Категории событий для ревизии

|  |  |
| --- | --- |
| Категория | События |
| 1 | 2 |
| Начало и конец сеанса | Попытки начала сеанса, попытки конца сеанса; создание и завершение сетевых соединений к серверу |
| Доступ к файлам и объектам | Доступы к каталогу или файлу, которые устанавливаются для ревизии в диспетчере файлов; использование принтера, управление компьютером |
| Использование прав пользователя | Успешное использование прав пользователя и неудачные попытки использовать права, не назначенные пользователям |
| Управление пользователями и группами | Создание, удаление и модификация учетных карточек пользователя и групп |
| Изменения полиса безопасности | Предоставление или отменена прав пользователя пользователям и группам, установка и разрыв связи доверия с другими доменами |
| Перезапуск, выключение и система | Остановка и перезапуск компьютера, заполнение контрольного журнала и отвержение данных проверки, если контрольный журнал уже полон |
| Трассировка процесса | Начало и остановка процессов в компьютере |

Для каждого пользователя предприятия обязательно устанавливаются свои права доступа к информации, разрешение на копирование и восстановление файлов.

5 Установка пароля и политика учетных карточек.

Для домена можно определить все аспекты политики пароля: минимальную длину пароля (по умолчанию 6 символов), минимальный и максимальный возраст пароля (по умолчанию устанавливается 14 и 30 дней) и исключительность пароля, который предохраняет пользователя от изменения его пароля на тот пароль, который пользователь использовал недавно (по умолчанию должен предохранить пользователей от повторного использования их последних трех паролей).

Дается возможность также определить и другие аспекты политики учетных карточек:

- должна ли происходить блокировка учетной карточки;

- должны ли пользователи насильно отключаться от сервера по истечении часов начала сеанса;

- должны ли пользователи иметь возможность входа в систему, чтобы изменить свой пароль.

Когда разрешена блокировка учетной карточки, тогда учетная карточка блокируется в случае нескольких безуспешных попыток начала сеанса пользователя, и не более чем через определенный период времени между любыми двумя безуспешными попытками начала сеанса. Учетные карточки, которые заблокированы, не могут быть использованы для входа в систему. Блокировка учетной карточки обязательно должна быть установлена в предприятие, что бы предотвратить попытки входа в систему.

Если пользователи принудительно отключаются от серверов, когда время его сеанса истекло, то они получают предупреждение как раз перед концом установленного периода сеанса. Если пользователи не отключаются от сети, то сервер произведет отключение принудительно. Часы сеанса в фирме установлены, так как недопустимо, чтобы сотрудники предприятия оставались на рабочем месте дольше установленного времени.

Если от пользователя требуется изменить пароль, то, когда он этого не сделал при просроченном пароле, он не сможет изменить свой пароль. При просрочке пароля пользователь должен обратиться к администратору системы за помощью в изменении пароля, чтобы иметь возможность снова входить в сеть. Если пользователь не входил в систему, а время изменения пароля подошло, то он будет предупрежден о необходимости изменения, как только он будет входить.

На предприятии доступ к сети Интернет имеют ограниченное число пользователей. При этом осуществляется защита вычислительных машин от вредоносных программ извне с помощью программного средства Антивирус Касперского Personal Pro, установленного на ЭВМ, имеющим доступ к сети Интернет.

 Разработанные рекомендации:

1. Так как на рабочие станции установлены операционные системы разных версий (Windows от 95 до ХР), то лучше устанавливать антивирусные программы на каждый компьютер. При этом почта будет проверяться на сервере (как это происходит в настоящий момент), а интернет-трафик – на каждой отдельной рабочей станции.

2. Установить программу контроля соблюдения правил работы на персональном компьютере.

3. Установить универсальный замок для защиты корпуса ПЭВМ, на которых производится обработка конфиденциальной информации, от несанкционированного вскрытия.

4. Установить систему санкционированного доступа на ПЭВМ, на которых производится обработка конфиденциальной информации. 4 Современные методы и средства аудита информационной безопасности

Сегодня не вызывает сомнений необходимость вложений в обеспечение информационной безопасности современного крупного бизнеса. Основной вопрос современного бизнеса - как оценить необходимый уровень вложений в ИБ для обеспечения максимальной эффективности инвестиций в данную сферу. Для решения этого вопроса существует только один способ - применять системы анализа рисков, позволяющие оценить существующие в системе риски и выбрать оптимальный по эффективности вариант защиты (по соотношению существующих в системе рисков к затратам на ИБ).

По статистике, самым большим препятствием на пути принятия каких-либо мер по обеспечению информационной безопасности в компании являются две причины:

- ограничение бюджета;

- отсутствие поддержки со стороны руководства.

Обе причины возникают из-за непонимания руководством серьезности вопроса и сложности задачи для ИТ-менеджера обосновать, зачем необходимо вкладывать деньги в информационную безопасность. Часто считается, что основная проблема заключается в том, что ИТ-менеджеры и руководители разговаривают на разных языках - техническом и финансовом, но ведь и самим ИТ-специалистам часто трудно оценить, на что потратить деньги и сколько их требуется для обеспечения большей защищенности системы компании, чтобы эти расходы не оказались напрасными или чрезмерными.

Если ИТ-менеджер четко представляет, сколько компания может потерять денег в случае реализации угроз, какие места в системе наиболее уязвимы, какие меры можно предпринять для повышения уровня защищенности и при этом не потратить лишних денег, и всё это подтверждено документально, то решение задачи убедить руководство обратить внимание и выделить средства на обеспечение информационной безопасности становится значительно более реальным.

Для решения данной задачи были разработаны программные комплексы анализа и контроля информационных рисков: британский CRAMM (компания Insight Consulting), американский RiskWatch (компания RiskWatch) и российский ГРИФ (компания Digital Security). Рассмотрим далее данные методы и построенные на их базе программные системы.

4.1 Метод CRAMM

Метод CRAMM (CCTA Risk Analysis and Managment Method) был разработан Агентством по компьютерам и телекоммуникациям Великобритании (Central Computer and Telecommunications Agency) по заданию Британского правительства и взят на вооружение в качестве государственного стандарта. Он используется, начиная с 1985 г , правительственными и коммерческими организациями Великобритании. За это время CRAMM приобрел популярность во всем мире. Фирма Insight Consulting Limited занимается разработкой и сопровождением одноименного программного продукта, реализующего метод CRAMM.

В настоящее время CRAMM - это довольно мощный и универсальный инструмент, позволяющий, помимо анализа рисков, решать также и ряд других аудиторских задач, включая:

- проведение обследования ИС и выпуск сопроводительной документации на всех этапах его проведения;

- проведение аудита в соответствии с требованиями Британского правительства, а также стандарта BS 7799:1995;

- разработка политики безопасности и плана обеспечения непрерывности бизнеса.

В основе метода CRAMM лежит комплексный подход к оценке рисков, сочетая количественные и качественные методы анализа. Метод является универсальным и подходит как для больших, так и для мелких организаций, как правительственного, так и коммерческого сектора. Версии программного обеспечения CRAMM, ориентированные на разные типы организаций, отличаются друг от друга своими базами знаний (profiles). Для коммерческих организаций имеется Коммерческий профиль (Commercial Profile), для правительственных организаций - Правительственный профиль (Government profile). Правительственный вариант профиля, также позволяет проводить аудит на соответствие требованиям американского стандарта ITSEC («Оранжевая книга»).

Грамотное использование метода CRAMM позволяет получать очень хорошие результаты, наиболее важным из которых, пожалуй, является возможность экономического обоснования расходов организации на обеспечение информационной безопасности и непрерывности бизнеса. Экономически обоснованная стратегия управления рисками позволяет, в конечном итоге, экономить средства, избегая неоправданных расходов.

CRAMM предполагает разделение всей процедуры на три последовательных этапа. Задачей первого этапа является ответ на вопрос: «Достаточно ли для защиты системы применения средств базового уровня, реализующих традиционные функции безопасности, или необходимо проведение более детального анализа?» На втором этапе производится идентификация рисков и оценивается их величина. На третьем этапе решается вопрос о выборе адекватных контрмер.

Методика CRAMM для каждого этапа определяет набор исходных данных, последовательность мероприятий, анкеты для проведения интервью, списки проверки и набор отчетных документов.

На первой стадии исследования производится идентификация и определение ценности защищаемых ресурсов.

Оценка производится по десятибалльной шкале, причем критериев оценки может быть несколько - финансовые потери, потери репутации и т.д.

При низкой оценке по всем используемым критериям (3 балла и ниже) считается, что рассматриваемая система требует базового уровня защиты (для этого уровня не требуется подробной оценки угроз ИБ) и вторая стадия исследования пропускается.

На второй стадии идентифицируются и оцениваются угрозы в сфере информационной безопасности, производится поиск и оценка уязвимостей защищаемой системы. Уровень угроз оценивается по следующей шкале: очень высокий, высокий, средний, низкий, очень низкий. Уровень уязвимости оценивается как высокий, средний или низкий. На основе этой информации вычисляется оценка уровня риска по семибальной шкале.

На третьей стадии CRAMM генерирует варианты мер противодействия выявленным рискам. Продукт предлагает рекомендации следующих типов:

- рекомендации общего характера;

- конкретные рекомендации;

- примеры того, как можно организовать защиту в данной ситуации.

CRAMM имеет обширную базу, содержащую описание около 1000 примеров реализации подсистем защиты различных компьютерных систем. Данные описания можно использовать в качестве шаблонов.

Решение о внедрении в систему новых механизмов безопасности и модификация старых принимает руководство организации, учитывая связанные с этим расходы, их приемлемость и конечную выгоду для бизнеса. Задачей аудитора является обоснование рекомендуемых контрмер для руководства организации.

В случае принятия решения о внедрении новых контрмер и модификации старых, на аудитора может быть возложена задача подготовки плана внедрения новых контрмер и оценки эффективности их использования. Решение этих задач выходит за рамки метода CRAMM.

К недостаткам метода CRAMM можно отнести следующее:

- использование метода CRAMM требует специальной подготовки и высокой квалификации аудитора;

- CRAMM в гораздо большей степени подходит для аудита уже существующих ИС, находящихся на стадии эксплуатации, нежели чем для ИС, находящихся на стадии разработки;

- аудит по методу CRAMM - процесс достаточно трудоемкий и может потребовать месяцев непрерывной работы аудитора;

- программный инструментарий CRAMM генерирует большое количество бумажной документации, которая не всегда оказывается полезной на практике;

- CRAMM не позволяет создавать собственные шаблоны отчетов или модифицировать имеющиеся;

- возможность внесения дополнений в базу знаний CRAMM не доступна пользователям, что вызывает определенные трудности при адаптации этого метода к потребностям конкретной организации;

- программное обеспечение CRAMM существует только на английском языке;

- стоимость лицензии от 2000 до 5000 долл.

4.2 Программное обеспечение RiskWatch

Программное обеспечение RiskWatch является мощным средством анализа и управления рисками. В семейство RiskWatch входят программные продукты для проведения различных видов аудита безопасности. Оно включает в себя следующие средства аудита и анализа рисков:

- RiskWatch for Physical Security - для физических методов защиты ИС;

- RiskWatch for Information Systems - для информационных рисков;

- HIPAA-WATCH for Healthcare Industry - для оценки соответствия требованиям стандарта HIPAA (US Healthcare Insurance Portability and Accountability Act);

- RiskWatch RW17799 for ISO 17799 - для оценки требованиям стандарта ISO 17799.

В методе RiskWatch в качестве критериев для оценки и управления рисками используются предсказание годовых потерь (Annual Loss Expectancy, ALE) и оценка возврата от инвестиций (Return on Investment, ROI).

Семейство программных продуктов RiskWatch имеет массу достоинств. RiskWatch помогает провести анализ рисков и сделать обоснованный выбор мер и средств защиты. Используемая в программе методика включает в себя 4 фазы.

В отличие от CRAMM, программа RiskWatch более ориентирована на точную количественную оценку соотношения потерь от угроз безопасности и затрат на создание системы защиты. Надо также отметить, что в этом продукте риски в сфере информационной и физической безопасности компьютерной сети предприятия рассматриваются совместно.

В основе продукта RiskWatch находится методика анализа рисков, которая состоит из четырех этапов.

Первый этап - определение предмета исследования. Здесь описываются такие параметры, как тип организации, состав исследуемой системы (в общих чертах), базовые требования в области безопасности. Для облегчения работы аналитика, в шаблонах, соответствующих типу организации ("коммерческая информационная система", "государственная/военная информационная система" и т.д.), есть списки категорий защищаемых ресурсов, потерь, угроз, уязвимостей и мер защиты. Из них нужно выбрать те, что реально присутствуют в организации.

Например, категории потерь:

- Задержки и отказ в обслуживании;

- Раскрытие информации;

- Прямые потери (например, от уничтожения оборудования огнем);

- Жизнь и здоровье (персонала, заказчиков и т.д.);

- Изменение данных;

- Косвенные потери (например, затраты на восстановление);

- Репутация.

Второй этап - ввод данных, описывающих конкретные характеристики системы. Данные могут вводиться вручную или импортироваться из отчетов, созданных инструментальными средствами исследования уязвимости компьютерных сетей.

На этом этапе:

1. Подробно описываются ресурсы, потери и классы инцидентов. Классы инцидентов получаются путем сопоставления категории потерь и категории ресурсов.

Для выявления возможных уязвимостей используется опросник, база которого содержит более 600 вопросов. Вопросы связаны с категориями ресурсов.

2. Задается частота возникновения каждой из выделенных угроз, степень уязвимости и ценность ресурсов. Все это используется в дальнейшем для расчета эффекта от внедрения средств защиты.

Третий и, наверное, самый важный этап - количественная оценка. На этом этапе рассчитывается профиль рисков, и выбираются меры обеспечения безопасности. Сначала устанавливаются связи между ресурсами, потерями, угрозами и уязвимостями, выделенными на предыдущих шагах исследования (риск описывается совокупностью этих четырех параметров).

Фактически, риск оценивается с помощью математического ожидания потерь за год. Например, если стоимость сервера $150000, а вероятность того, что он будет уничтожен пожаром в течение года, равна 0.01, то ожидаемые потери составят $1500.

Общеизвестная формула (m=p\*v , где m-математическое ожидание, p - вероятность возникновения угрозы, v - стоимость ресурса) претерпела некоторые изменения, в связи с тем, что RiskWatch использует определенные американским институтом стандартов NIST оценки, называемые LAFE и SAFE. LAFE (Local Annual Frequency Estimate) - показывает, сколько раз в год в среднем данная угроза реализуется в данном месте (например, в городе). SAFE (Standard Annual Frequency Estimate) - показывает, сколько раз в год в среднем данная угроза реализуется в этой "части мира" (например, в Северной Америке). Вводится также поправочный коэффициент, который позволяет учесть, что в результате реализации угрозы защищаемый ресурс может быть уничтожен не полностью, а только частично.

Дополнительно рассматриваются сценарии "что если", которые позволяют описать аналогичные ситуации при условии внедрения средств защиты. Сравнивая ожидаемые потери при условии внедрения защитных мер и без них можно оценить эффект от таких мероприятий.

RiskWatch включает в себя базы с оценками LAFE и SAFE, а также с обобщенным описанием различных типов средств защиты.

Четвертый этап - генерация отчетов. Типы отчетов:

1. Краткие итоги.

2. Полные и краткие отчеты об элементах, описанных на стадиях 1 и

3. Отчет от стоимости защищаемых ресурсов и ожидаемых потерях от реализации угроз.

4. Отчет об угрозах и мерах противодействия.

5. Отчет о результатах аудита безопасности.

Таким образом, рассматриваемое средство позволяет оценить не только те риски, которые сейчас существуют у предприятия, но и ту выгоду, которую может принести внедрение физических, технических, программных и прочих средств и механизмов защиты. Подготовленные отчеты и графики дают материал, достаточный для принятия решений об изменении системы обеспечения безопасности предприятия.

Для отечественных пользователей проблема заключается в том, что получить используемые в RiskWatch оценки (такие как LAFE и SAFE) для наших условий достаточно проблематично. Хотя сама методология может с успехом применяться и у нас.

Подводя итог, можно отметить, что конкретную методику проведения анализа рисков на предприятии и инструментальные средства, поддерживающие ее, нужно выбирать, учитывая следующие факторы:

1. Наличие экспертов, способных дать достоверные оценки объема потерь от угроз информационной безопасности;

2. Наличие на предприятии достоверной статистки по инцидентам в сфере информационной безопасности;

3. Нужна ли точная количественная оценка последствий реализации угроз или достаточно оценки на качественном уровне.

К недостаткам RiskWatch можно отнести:

1. Такой метод подходит, если требуется провести анализ рисков на программно-техническом уровне защиты, без учета организационных и административных факторов.

2. Полученные оценки рисков (математическое ожидание потерь) далеко не исчерпывает понимание риска с системных позиций - метод не учитывает комплексный подход к информационной безопасности.

3. Программное обеспечение RiskWatch существует только на английском языке.

4. Высокая стоимость лицензии (от 10 000 долл. за одно рабочее место для небольшой компании).

4.3 Комплексная система анализа и управления рисками ГРИФ

ГРИФ - комплексная система анализа и управления рисками информационной системы компании. ГРИФ 2005 из состава Digital Security Office дает полную картину защищенности информационных ресурсов в системе и позволяет выбрать оптимальную стратегию защиты информации компании.

Система ГРИФ:

1. Анализирует уровень защищенности всех ценных ресурсов компании

2. Оценивает возможный ущерб, который понесет компания в результате реализации угроз информационной безопасности

3. Позволяет эффективно управлять рисками при помощи выбора контрмер, наиболее оптимальных по соотношению цена/качество

Как работает система ГРИФ:

Система ГРИФ 2005 предоставляет возможность проводить анализ рисков информационной системы при помощи анализа модели информационных потоков, а также, анализируя модель угроз и уязвимостей - в зависимости от того, какими исходными данными располагает пользователь, а также от того, какие данные интересуют пользователя на выходе.

Модель информационных потоков

При работе с моделью информационных потоков в систему вносится полная информация обо всех ресурсах с ценной информацией, пользователях, имеющих доступ к этим ресурсам, видах и правах доступа. Заносятся данные обо всех средствах защиты каждого ресурса, сетевые взаимосвязи ресурсов, а также характеристики политики безопасности компании. В результате получается полная модель информационной системы.

Шаг 1.

На первом этапе работы с программой пользователь вносит все объекты своей информационной системы: отделы, ресурсы (специфичными объектами данной модели являются сетевые группы, сетевые устройства, виды информации, группы пользователей, бизнес-процессы).

Шаг 2.

Далее пользователю необходимо проставить связи, т.е. определить к каким отделам и сетевым группам относятся ресурсы, какая информация хранится на ресурсе, и какие группы пользователей имеют к ней доступ. Также пользователь системы указывает средства защиты ресурса и информации.

Шаг 3.

На завершающем этапе пользователь отвечает на список вопросов по политике безопасности, реализованной в системе, что позволяет оценить реальный уровень защищенности системы и детализировать оценки рисков.

Наличие средств информационной защиты, отмеченных на первом этапе, само по себе еще не делает систему защищенной в случае их неадекватного использования и отсутствия комплексной политики безопасности, учитывающей все аспекты защиты информации, включая вопросы организации защиты, физической безопасности, безопасности персонала, непрерывности ведения бизнеса и т.д.

В результате выполнения всех действий по данным этапам, на выходе сформирована полная модель информационной системы с точки зрения информационной безопасности с учетом реального выполнения требований комплексной политики безопасности, что позволяет перейти к программному анализу введенных данных для получения комплексной оценки рисков и формирования итогового отчета.

Модель угроз и уязвимостей

Работа с моделью анализа угроз и уязвимостей подразумевает определение уязвимостей каждого ресурса с ценной информацией, и подключение соответствующих угроз, которые могут быть реализованы через данные уязвимости. В результате получается полная картина того, какие слабые места есть в информационной системе и тот ущерб, который может быть нанесен.

Шаг 1.

На первом этапе работы с продуктом пользователь вносит объекты своей информационной системы: отделы, ресурсы (специфичными объектами для данной модели: угрозы информационной системы, уязвимости, через которые реализуются угрозы).

Система ГРИФ 2005 содержит обширные встроенные каталоги угроз и уязвимостей. Для достижения максимальной полноты и универсальности данных каталогов, экспертами Digital Security была разработана специальная классификация угроз, в которой реализован многолетний практический опыт в области информационной безопасности. Используя каталоги угроз и уязвимостей, пользователь может выбрать угрозы и уязвимости, относящиеся к его информационной системе. Каталоги содержат около 100 угроз и 200 уязвимостей.

Шаг 2.

Далее пользователю необходимо проставить связи, т.е. определить к каким отделам относятся ресурсы, какие угрозы действуют на ресурс и через какие уязвимости они реализуются.

Алгоритм системы ГРИФ 2005 анализирует построенную модель и генерирует отчет, который содержит значения риска для каждого ресурса. Конфигурации отчета может быть практически любой, таким образом, позволяя пользователю создавать как краткие отчеты для руководства, так и детальные отчеты для дальнейшей работы с результатами.

Система ГРИФ 2005 содержит модуль управления рисками, который позволяет проанализировать все причины того значения риска, который получается после обработки алгоритмом занесенных данных. Таким образом, зная причины, Вы будете обладать всеми данными, необходимыми для реализации контрмер и, соответственно, снижения уровня риска. Благодаря расчету эффективности каждой возможной контрмеры, а также определению значения остаточного риска, Вы сможете выбрать наиболее оптимальные контрмеры, которые позволят снизить риск до необходимого уровня с наименьшими затратами.

В результате работы с системой ГРИФ строится подробный отчет об уровне риска каждого ценного ресурса информационной системы компании, все причины риска с подробным анализом уязвимостей и оценкой экономической эффективности всех возможных контрмер.

Лучшие мировые практики и ведущие международные стандарты в области информационной безопасности, в частности ISO 17799, требуют для эффективного управления безопасностью информационной системы внедрения системы анализа и управления рисками.

При этом можно использовать любые удобные инструментальные средства, но, главное - всегда четко понимать, что система информационной безопасности создана на основе анализа информационных рисков, проверена и обоснована. Анализ и управление информационными рисками - ключевой фактор для построения эффективной защиты информационной системы.

## 5 Охрана труда и безопасность жизнедеятельности

## 5.1 Охрана труда

Охрана труда – система законодательных актов, постановлений, организационных, санитарных и технических мер, обеспечивающих безопасные для здоровья условия труда на рабочем месте. Научно-технический прогресс внес изменения в условия производственной деятельности работников умственного труда. Их труд стал более интенсивным, напряженным, требующим затрат умственной, эмоциональной и физической энергии. Это имеет прямое отношение и к специалистам, связанным с проектированием, разработкой, эксплуатацией, сопровождением и модернизацией автоматизированных систем управления различного назначения.

На рабочем месте специалиста по ИБ должны быть созданы условия для высокопроизводительного труда. Специалиста по ИБ АРМ испытывает значительную нагрузку, как физическую (сидячее положение, нагрузка на глаза), так и умственную, что приводит к снижению его трудоспособности к концу рабочего дня.

Существуют нормативы, определяющие комфортные условия и предельно допустимые нормы запыленности, температуры воздуха, шума, освещенности. В системе мер, обеспечивающих благоприятные условия труда, большое место отводится эстетическим факторам: оформление производственного интерьера, оборудования, применение функциональной музыки и др., которые оказывают определенное воздействие на организм человека. Важную роль играет окраска помещений, которая должна быть светлой. В данном разделе дипломного проекта рассчитывается необходимая освещенность рабочего места и информационная нагрузка специалиста по ИБ.

Развитию утомляемости на производстве способствуют следующие факторы:

* неправильная эргономическая организация рабочего места, нерациональные зоны размещения оборудования по высоте от пола, по фронту от оси симметрии и т.д.;
* характер протекания труда.

Трудовой процесс организован таким образом, что специалиста по ИБ вынужден с первых минут рабочего дня решать наиболее сложные и трудоемкие задачи, в то время как в первые минуты работы функциональная подвижность нервных клеток мозга низка. Важное значение имеет чередование труда и отдыха, смена одних форм работы другими.

Одним из основных вопросов охраны труда является организация рационального освещения производственных помещений и рабочих мест.

Для освещения помещения, в котором работает специалиста по ИБ, используется смешанное освещение, т.е. сочетание естественного и искусственного освещения.

Естественное освещение – осуществляется через окна в наружных стенах здания.

Искусственное освещение – используется при недостаточном естественном освещении и осуществляется с помощью двух систем: общего и местного освещения. Общим называют освещение, светильники которого освещают всю площадь помещения. Местным называют освещение, предназначенное для определенного рабочего места.

Для помещения, где находится рабочее место оператора, используется система общего освещения.

Нормами для данных работ установлена необходимая освещенность рабочего места ЕН=300 лк (для работ высокой точности, когда наименьший размер объекта различения равен 0.3 – 0.5 мм).

Для исключения засветки экранов дисплеев прямыми световыми потоками светильники общего освещения располагают сбоку от рабочего места, параллельно линии зрения оператора и стене с окнами.

Кроме того, необходимо в течение 8-ми часового рабочего дня предусмотреть один часовой перерыв на обед, 5-ти минутные перерывы каждые полчаса и 15-ти минутные перерывы каждые 1.5 – 2 часа. Работу необходимо организовать таким образом, чтобы наиболее сложные задачи решались с 11:00 до 16:00 – в период наибольшей активности человека, а не в начале дня, когда оператор еще не достиг максимальной активности, и не в конце дня, когда уже развивается утомление.

Так как работа специалиста по ИБ не связана с решением крупных логических задач и достаточно однообразна, то рекомендуется по возможности чередовать виды деятельности.

5.2 Безопасность жизнедеятельности

Важным моментом в комплексе мероприятий направленных на совершенствование условий труда являются мероприятия по охране труда. Этим вопросам с каждым годом уделяется все большее внимание, т.к. забота о здоровье человека стала не только делом государственной важности, но и элементом конкуренции работодателей в вопросе привлечения кадров. Для успешного воплощения в жизнь всех мероприятий по охране труда необходимы знания в области физиологии труда, которые позволяют правильно организовать процесс трудовой деятельности человека.

В данном разделе дипломного проекта освещаются основные вопросы техники безопасности и экологии труда.

Состояние условий труда студента и его безопасности, на сегодняшний день, еще не удовлетворяют современным требованиям.

Студент сталкиваются с воздействием таких физически опасных и вредных производственных факторов, как повышенный уровень шума, повышенная температура внешней среды, отсутствие или недостаточная освещенность рабочей зоны, электрический ток, статическое электричество и другие.

Многие студенты связаны с воздействием таких психофизических факторов, как умственное перенапряжение, перенапряжение зрительных и слуховых анализаторов, монотонность труда, эмоциональные перегрузки. Воздействие указанных неблагоприятных факторов приводит к снижению работоспособности, вызванное развивающимся утомлением. Появление и развитие утомления связано с изменениями, возникающими во время работы в центральной нервной системе, с тормозными процессами в коре головного мозга.

Медицинские обследования студентов показали, что помимо снижения производительности труда высокие уровни шума приводят к ухудшению слуха. Длительное нахождение человека в зоне комбинированного воздействия различных неблагоприятных факторов может привести к профессиональному заболеванию.

6 Экономическое обоснование

6.1 Расчет капитальных вложений

6.1.1 Капитальные вложения, необходимые для реализации данного проекта, определяются по формуле (1):

К=Кобор+Кт (1)

где Кобор – стоимость оборудования;

Кт – транспортные и заготовительно-складские расходы;

6.1.2 Расчет стоимости оборудования показан в таблице 3:

Таблица 3 – Расчет стоимости оборудования

|  |  |  |  |
| --- | --- | --- | --- |
| Наименования | Количество, шт | Цена, руб. | Сумма, руб. |
| Монитор | 1 | 6 880 | 6 880 |
| Системный блок | 1 | 12 390 | 12 390 |
| Мышь | 1 | 230 | 230 |
| Клавиатура | 1 | 520 | 520 |
| ПО RiskWatch | 1 | 25 000 | 25 000 |
| ПО ViPNet | 1 | 20 000 | 20 000 |
| Антивирус Kaspersky | 1 | 1 800 | 1 800 |
| Итого:  |  |  | 66 820 |

6.1.3 Определяем транспортные и заготовительно-складские расходы:

Кт=66 820\*0,05=3 341 руб.

6.1.4 Определяем величину капитальных затрат:

К=66 820+3 341=70 161 руб.

Таблица 4 – Величина капитальных затрат:

|  |  |  |
| --- | --- | --- |
| Наименование показателей | Ед. измерения | Стоимостная оценка |
| Стоимость оборудования | руб. | 66 820 |
| Транспортные и заготовительно-складские расходы | руб. | 3 341 |
| Итого: |  | 70 161 |

6.2 Расчет расходов

В процессе разработки осуществляется деятельность, требующая расходов ресурсов. Сумма составит фактическую себестоимость или величину расходов на разработку, включая следующие статьи расходов:

6.2.1 Затраты на оплату труда

Определяем сумму зарплаты по формуле (2):

Зпл= окл\*n\*Rпрем, (2)

где окл – оклад специалиста;

n – количество месяцев на разработку проекта;

R – коэффициент учитываемой премии

Зпл=20 000\*1\*1,3=26 000 руб.

Определяем сумму налоговых платежей от з/пл.

Отчисления на соц. нужды определяются по формуле (3):

 ЕСН=з/пл\*Сесн/100%, (3)

где ЕСН – единый соц. налог;

 з/пл – оплата труда;

 Сесн – ставка единого соц. налога.

ЕСН=26 000\*0,26=6 760 руб.

6.2.2 Амортизационные отчисления

Предполагается, что оборудование будет эксплуатироваться в течении трех лет без модернизации и демонтажа. Таким образом, срок эксплуатации будет равен трем годам, следовательно:

Нагод=100/3=33,3%,

 Амес=к\*На/100\*n, (4)

где к – стоимость оборудования;

На – амортизационные нормы;

n – количество месяцев.

Амес=70 161\*33,3/100\*12=1 947 руб.

6.2.3 Оплата электроэнергии, используемой оборудованием

При разработке проекта используется электроэнергия, расходы на которую определяются с учетом времени действия компьютера, тарифа за электроэнергию и мощности используемой техники.

Мощность компьютера – 0.2 кВт

Время работы компьютера – 45 часов

Тариф за 1 кВт – 2,71 руб.

Расходы на электроэнергию рассчитываются по формуле (5):

 Рэл/эн=Т\*t\*n\*W, (5)

где Т – тариф на электроэнергию;

t – время работы в день;

n – количество дней;

W – потребляемая мощность единицы оборудования в час.

Рэл/эн=2,71\*8\*25\*0,3=162,6 руб.

6.2.4 Прочие расходы

Сумму прочих расходов примем в размере 0,1% от стоимости оборудования:

 Рпроч=К\*0,1%/100%, (6)

Рпроч=70 161\*0,1%/100%=70,161 руб.

6.2.5 Общая сумма эксплуатационных расходов показана в таблице 5:

Таблица 5 – Сумма эксплуатационных расходов

|  |  |
| --- | --- |
| Статьи затрат | Сумма затрат, руб. |
| Расходы на оплату труда | 26 000 |
| ЕСН | 6 760 |
| Амортизационные отчисления | 1 947 |
| Оплата электроэнергии | 162,6 |
| Прочие расходы | 70,161 |
| Итого: | 34 939,761 |

6.2.6 Расчет удельного веса расходов

 dn=Pn/∑P\*100% (7)

где dn – удельный вес расходов;

Рn – рассчитываемые капитальные статьи;

∑P – сумма расходов.

dРОТ=26 000/34 939,761\*100=74,41%.

dЕСН=6 766/ 34 939,761\*100=19,36%.

dА=1 947/34 939,761\*100=5,57%.

dЗ на Эл=162,6/34 939,761\*100=0,47%.

dпроч. р=70,161/34 939,761\*100=0,2%.

Общая сумма удельного веса расходов показана в таблице 6:

Таблица 6 – Общая сумма удельного веса

|  |  |
| --- | --- |
| Наименование статей расходов | Удельный вес, % |
| dРОТ | 74,41 |
| dЕСН | 19,36 |
| dА | 5,57 |
| dЗ на Эл | 0,47 |
| dпроч. р | 0,2 |
| Итого: | 100 |

Таким образом, рассчитав смету затрат на разработку технологий аудита, можно сделать вывод, что затраты на его изготовление составили 34 939,761 рублей.

Заключение

В результате реализации дипломного проекта был проведен анализ системы защиты информации предприятия ОАО «РОСТСТРОЙ», выявивший ряд ее недостатков, оставляющих возможность реализации угроз целостности, доступности и достоверности информации, циркулирующей в организации. На основе выявленных недостатков был разработан и внедрен профиль защиты, заключающийся в комплексе требований к организации защиты информации, реализация которых позволит модернизировать систему защиты и пресечь возможные каналы утечки информации. Данный комплекс требований охватывает все значимые составляющие системы информационной безопасности организации и подразумевает введение в эксплуатацию новых программных и аппаратных средств защиты информации, каждое из которых позволит снизить риски утечки на своем участке ответственности, формируя комплексную надежную систему защиты.

В соответствии с предложенным в дипломном проекте комплексным подходом к защите информации рассмотрена многоуровневая система безопасности, включающая в себя:

 - средства защиты рабочих мест и серверов ИТС;

 - средства защиты сетевых устройств (коммутаторы и маршрутизаторы);

 - межсетевые экраны;

 - средства антивирусной защиты, интегрированные как в рабочие места, так и серверы, и межсетевые экраны;

 - средства криптографической защиты информации как передаваемой по каналам связи, так и хранимой на рабочих местах и серверах.

В заключение можно сказать, что задачи дипломного проекта были выполнены в полной мере, а произведенная модификация системы защиты информации организации соответствует всем предъявленным к ней требованиям.

Список литературы

## 1. Ф. Даниловский. Информационная безопасность банковских систем. Финансовая газета, N 34, август 2003 г.

## 2. Федеральный закон РФ от 20 февраля 1995 г. Об информации, информатизации и защите информации. № 24 – ФЗ. (с изменениями от 10.01.2003).

## 3. Гостехкомиссия России. Руководящий документ. Защита от несанкционированного доступа к информации. М., 1992 г.

## 4. Гостехкомиссия России. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. М., 1992 г.

## 5. Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. М., 1992 г.

## 6. Гостехкомиссия России. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. М., 1997 г.

## 7. Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. М., 1997 г.

## 8. Гостехкомиссия России. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. М., 1999 г

## 9. Банк России. Положение об организации внутреннего контроля в кредитных организациях и банковских группах. 16 декабря 2003 г. № 242-П.

Приложение А

Инструкция по обеспечению сохранности коммерческих тайн на предприятии

1 Общие положения

1. Настоящая инструкция разработана в соответствии с требованиями законов РФ и предусматривает административные и экономические меры защиты коммерческой тайны предприятия с целью предотвращения нанесения возможного экономического и морального ущерба предприятию со стороны юридических и физических лиц, вызванного их неправомерными или не осторожными действиями путем безвозмездного присвоения чужой информации или разглашения коммерческой тайны.

2. Под коммерческой тайной предприятия понимаются не являющиеся государственными секретами сведения, связанные с производством, технологической информацией, управлением, финансами и другой деятельностью предприятия, разглашение (передача, утечка) которых может нанести ущерб его интересам. К сведениям, составляющим коммерческую тайну, относятся несекретные сведения, предусмотренные "Перечнем сведений, составляющих коммерческую тайну предприятия", утвержденным и введенным в действие приказом руководителя предприятия. Коммерческая тайна предприятия является его собственностью. Если она представляет собой результат совместной деятельности с другими предприятиями, основанной на договорных началах, то коммерческая тайна может быть собственностью двух сторон, что должно найти отражение в договоре.

3. Под разглашением коммерческой тайны подразумевается умышленные или неосторожные действия должностных или иных физических лиц, приведшие к не вызванному служебной необходимостью или преждевременному открытому опубликованию сведений, подпадающих под категорию сведений, составляющих коммерческую тайну, а также передача подобных сведений по открытым техническим каналам связи или их обработка на некатегорированных СВТ.

4. Под открытым опубликованием таких сведений подразумевается их публикация в открытой печати, передача по радио и телевидению, оглашение на международных, зарубежных и открытых внутрироссийских симпозиумах, совещаниях, конференциях, съездах, при публичных вступлениях и защите диссертаций, вывоз материалов за границу или передача их в любой форме иностранным фирмам, организациям или отдельным лицам.

5. Необходимость открытого опубликования сведений, составляющих коммерческую тайну, их объемы, формы и время опубликования определяются руководителем предприятия с учетом заключения постоянно действующей экспертной комиссии.

6. Использование для открытого опубликования сведений, полученных на договорной или доверительной основе или являющихся результатом совместной деятельности, допускается только с общего согласия партнеров.

7. Меры по ограничению открытых публикаций коммерческой информации не могут быть использованы для сокрытия от общественности фактов злоупотреблений, расточительства, бесхозяйственности, недобросовестной конкуренции и других негативных явлений в деятельности предприятия.

8. Передача информации сторонним организациям, с которыми предприятие не связано прямыми служебными контактами, должна регулироваться, как правило, договорными отношениями, предусматривающими обязательства и ответственность пользователей, включая возмещение материальных затрат за предоставление информации и компенсацию за нарушение договорных обязательств.

9. Тиражированные документы и издания с грифом «КОММЕРЧЕСКАЯ ТАЙНА» («КТ») рассматриваются как материалы, содержащие сведения ограниченного распространения.

10. Защита коммерческой тайны предусматривает:

- порядок определения информации, содержащей коммерческую тайну, и сроков ее действия;

- систему допуска сотрудников предприятия, частных и командированных лиц к сведениям, составляющим коммерческую тайну предприятия;

- обязанности лиц, допущенных к таким сведениям;

- порядок работы с документами, имеющими гриф «КТ»;

- обеспечение сохранности документов, дел и изданий с грифом «КТ»;

- принципы организации и проведения контроля за обеспечением установленного порядка при работе со сведениями, составляющими коммерческую тайну;

- ответственность за разглашение сведений и утрату документов, содержащих коммерческую тайну.

11. Ответственность за организацию работы с материалами, имеющими гриф «КТ», разработку и осуществление необходимых мер по сохранности коммерческой тайны руководитель предприятия возлагает на ответственных руководителей направлений и структурных подразделений

12. Контроль за осуществлением мер, обеспечивающих сохранность коммерческой тайны, возлагается на службу информационной безопасности предприятия, которая контролирует, а в необходимых случаях обеспечивает учет, размножения и хранения документов, дел и изданий с грифом коммерческая тайна»; обеспечивает сохранность коммерческой тайны путем максимального ограничения круга лиц, допущенных к коммерческой тайне предприятия, выполнение требований при обработке информации с грифом «КТ» на защищенных СВТ, а также требований по конфиденциальности конкретной информации, внесенных в договора со сторонними предприятиями – партнерами.

2 Определение информации и обозначение документов, содержащих коммерческую тайну, и сроков ее действия

1. Необходимость проставления грифа «Коммерческая тайна» («КТ») определяется в соответствии с Перечнем, указанным в п.1.2 настоящей Инструкции: при работе с документом-исполнителем и лицом, подписывающим документ, при работе с изданием-автором (составителем) и руководителем, утверждающим издание к печати.

2. На документах, делах и изданиях, содержащих сведения, составляющие коммерческую тайну, проставляется гриф «Коммерческая тайна» («КТ»), а на документах и изданиях, кроме того, – номера экземпляров. Гриф и номера экземпляров, проставляются в правом верхнем углу первой страницы документа, на обложке или титульном листе издания и на первой странице сопроводительного письма к этим материалам. На обратной стороне последнего листа каждого экземпляра печатается разметка, в которой указывается: количество отпечатанных экземпляров, номер, фамилия исполнителя и его телефон, дата, фамилия машинистки и срок действия коммерческой тайны (регистрационный номер проставляется на каждом листе документа).

3. Срок действия коммерческой тайны, содержащейся в документе, определяется в каждом конкретном случае исполнителем или лицом, подписавшем документ, в виде конкретной даты или в виде пометок: «до заключения контракта», «бессрочно» и т.п.

4. Основанием для снятия грифа «Коммерческая тайна» является решение постоянно действующей экспертной комиссии, оформляемым актом, утвержденным руководителем предприятия. К работе комиссии привлекаются представители заинтересованных структурных подразделений. Один экземпляр акта вместе с делами передается в архив предприятия, а на деле постоянного хранения в государственных архив.

5. Гриф «КТ» после оформления его снятия (п. 2.4) погашается штампом или записью о руки с указанием даты и номера акта, послужившего основанием для его снятия. Аналогичные отметки вносятся в описи и номенклатуры дел.

3 Организация работы с документами, имеющими гриф «Коммерческая тайна» («КТ»)

1. Документы, имеющие гриф «КТ», подлежат обязательной регистрации в подразделении делопроизводства службы информационной безопасности. Эти документы должны иметь реквизиты, предусмотренные п.2.2 и гриф «КТ» (или полностью «Коммерческая тайна»).

Права на информацию, порядок пользования ею, сроки ограничения на публикацию могут оговариваться дополнительно в тексте документа и его реквизитах.

Отсутствие грифа «КТ» и предупредительных оговорок в тексте и реквизитах означает свободную рассылку и предполагает, что автор информации и лицо, подписавшее или утвердившее документ, предусмотрели возможные последствия от свободной рассылки и несут за это ответственность.

2. Вся поступающая корреспонденция, имеющая гриф «КТ» (или другие соответствующие этому понятию грифы, например, «секрет предприятия, «тайна предприятия» и др.) принимается и вскрывается сотрудниками предприятия, которым поручена работа с этими материалами. При этом проверяется количество листов и экземпляров, а также наличие указанных в сопроводительном письме приложений. При обнаружении отсутствия в конвертах (пакетах) указанных документов составляется акт в двух экземплярах: один экземпляр акта направляется отправителю.

3. Все входящие, исходящие и внутренние документы, а также издания с грифом «КТ» подлежат регистрации и учитываются по количеству листов, а издания – поэкземплярно.

4. Учет документов и изданий с грифом «КТ» ведется в журналах или карточках отдельно от учета другой служебной несекретной документации. Листы журналов нумеруются, прошиваются и опечатываются. Документы, которые не подшиваются в дела, учитываются в журнале инвентарного учета.

Движение документов и изданий с грифом «КТ» своевременно отражается в журналах или карточках.

5. На зарегистрированном документе с грифом «КТ» (или на сопроводительном листе к изданиям с грифом «КТ») должен быть проставлен штамп с указанием наименования предприятия, регистрационный номер документа и дата его поступления.

6. Издания с грифом «КТ» регистрируются в журнале учета и распределения изданий.

7. Отпечатанные и подписанные документы вместе с их черновиками передаются для регистрации сотруднику подразделения делопроизводства службы информационной безопасности, осуществляющему их учет. Черновики уничтожаются исполнителем и этим сотрудником, что подтверждается росписью указанных лиц в журнале или на карточках учета. При этом проставляется дата и подпись.

8. Размножение документов и изданий с грифом «КТ» в типографиях и других множительных участках производится с разрешения и под контролем специально назначенных сотрудников службы информационной безопасности по заказам, подписанным руководителем предприятия.

Размноженные документы «КТ» (копии, тираж) должны быть полистно подобраны, пронумерованы поэкземплярно и, при необходимости, сброшюрованы (сшиты). Нумерация дополнительно размноженных экземпляров, производится от последнего номера, ранее учтенных экземпляров этого документа.

Перед размножением на последнем листе оригинала (подлинника) проставляется запись: «Регистрационный номер. Дополнительно размножено \_ экз., на \_ листах текста. Наряд N \_ от \_\_\_. Подпись (исполнитель заказа)». Одновременно делается отметка об этом в соответствующих журналах и карточках учета.

9. Рассылка документов и изданий с грифом «КТ» производиться на основании подписанных руководителем структурного подразделения разнарядок с указанием учетных номеров отправляемых экземпляров.

Пересылка пакетов с грифом «КТ» может осуществляться через органы спецсвязи или фельдсвязи.

10. Документы с грифом «КТ» после исполнения группируются в отдельные дела. Порядок их группировки предусматривается специальной номенклатурой дел, в которую в обязательном порядке включаются все справочные картотеки и журналы на документы и издания с грифом «КТ».

11. Снятия рукописных, машинописных, микро- и фотокопий, электрографических и др. копий, а также производство выписок из документов и изданий с грифом «КТ» сотрудниками предприятия производится по разрешению руководителя предприятия и подразделений.

12. Обработка информации с грифом «КТ» производится на учетных СВТ, которые имеют категорию не ниже 4-Б.

4 Порядок обеспечения сохранности документов, дел и изданий

1. Все имеющие гриф «КТ» документы, дела и издания должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах. Помещения должны отвечать требованиям внутриобъектового режима, обеспечивающего физическую сохранность находящейся в них документации.

2. Дела с грифом «КТ», выдаваемые исполнителю, подлежат возврату в подразделение делопроизводства службы информационной безопасности (СИБ) в тот же день. При необходимости, с разрешения начальника подразделения делопроизводства СИБ или уполномоченного СИБ они могут находиться у исполнителя в течение срока, необходимого для выполнения задания, при условии полного обеспечения их сохранности и соблюдения правил хранения.

3. С документацией с грифом «КТ» разрешается работать только в служебных помещениях. Для работы вне служебных помещений необходимо разрешение руководителя предприятия или структурного подразделения.

4. Документы, дела и издания с грифом «КТ» могут передаваться другим сотрудникам, допущенным к этим документам, только через делопроизводство СИБ или уполномоченного СИБ.

5. Изъятия из дел или перемещение документов с грифом «КТ» из одного дела в другое без санкции руководителя делопроизводства СИБ или уполномоченного СИБ, осуществляющего их учет, запрещается.

6. Смена сотрудников, ответственных за учет и хранение документов, дел и изданий с грифом «КТ», оформляется распоряжением начальника подразделения. При этом составляется по произвольной форме акт приема-передачи этих материалов, утверждаемый указанным руководителем.

7. Уничтожение документов «КТ» производится комиссией в составе не менее трех человек с составлением акта.

8. Печатание документов «КТ» разрешается в машинописном бюро или непосредственно в подразделениях. Для учета отпечатанных документов ведется специальный журнал.

5 Порядок допуска к сведениям, составляющим коммерческую тайну предприятия

1. Допуск сотрудников к сведениям, составляющим коммерческую тайну, осуществляется руководителем предприятия или руководителями его структурных подразделений.

Руководители подразделений и службы информационной безопасности обязаны обеспечить систематический контроль за допуском к этим сведениям только тех лиц, которым они необходимы для выполнения служебных обязанностей.

2. К сведениям, составляющим коммерческую тайну, допускаются лица, личные и деловые качества которых обеспечивают их способность хранить коммерческую тайну, и только после оформления в службе информационной безопасности письменного обязательства по сохранению коммерческой тайны.

3. Допуск сотрудников к работе с делами «КТ» осуществляется согласно оформленному не внутренней стороне обложки дела или на отдельном листе списку за подписью руководителя предприятия структурного подразделения, а к документам – в соответствии с указаниями, содержащимися в резолюциях руководителей предприятия и подразделений.

4. Представители сторонних организаций и частные лица могут быть допущены к ознакомлению и работе с документами и изданиями с грифом «КТ» с письменного разрешения руководителей предприятия или подразделений, в ведении которых находятся эти материалы.

Выписки из документов и изданий, содержащих сведения с грифом «КТ», производятся в блокнотах (или тетрадях), которые имеют такой же гриф. После окончания работы они высылаются в адрес той организации, которая будет указана данным представителем.

5. Выдача дел и изданий с грифом «КТ» исполнителям и прием от них производится под расписку в «Карточке учета выдаваемых дел и изданий».

Дела и издания непосредственно представителям сторонних организаций и частным лицам не выдаются. При необходимости с их содержанием они ознакомятся только с разрешения руководителя предприятия через уполномоченного службы информационной безопасности или представителя заинтересованного подразделения.

6 Контроль выполнения требований внутриобъектового режима при работе со сведениями, содержащими коммерческую тайну

1. Под внутри объектовым режимом при работе с коммерческой тайной подразумевается соблюдение условий работы, исключающих возможность утечки информации о сведениях, содержащих коммерческую тайну.

2. Контроль соблюдения указанного режима осуществляется в целях изучения и оценки состояния сохранности коммерческой тайны, выявления и установления причин недостатков, и выработки предложений по их устранению.

3. Контроль обеспечения режима при работе со сведениями, содержащими коммерческую тайну, осуществляют служба информационной безопасности предприятия и руководитель структурного подразделения путем текущих и плановых проверок.

4. При проведении проверок создается комиссия, которая комплектуется из опытных и квалифицированных работников в составе не менее двух человек, допущенных к работе с материалами «КТ».

Участие в проверке не должно приводить к необоснованному увеличению осведомленности в этих сведениях.

5. Плановые проверки проводятся не реже одного раза в год комиссиями на основании приказа или распоряжения руководителя предприятия (подразделения).

6. Проверяющие имеют право знакомиться со всеми документами, журналами (карточками) и другими материалами, имеющими отношение к проверяемым вопросам, а также проводить беседы, консультироваться со специалистами и исполнителями, требовать представления письменных объяснений, справок и отчетов по всем вопросам, входящим в компетенцию комиссии.

7. При проверках присутствует руководитель структурного подразделения или его заместитель.

8. По результатам проверок составляется акт или справка с отражением в нем наличия документов, состояния работы с материалами «КТ», выявленных недостатков и предложений по их устранению. Акт утверждается руководителем предприятия (подразделения).

9. При выявлении случаев утраты документов или разглашения сведений, составляющих коммерческую тайну, ставятся в известность руководитель предприятия и его заместитель (помощник) по безопасности. Для расследования указанных случаев приказом руководителя предприятия создается комиссия, которая определяет соответствие содержания утраченного документа проставленному грифу «КТ» и выявляет обстоятельства утраты (разглашения). По результатам работы комиссии составляется акт.

7 Обязанности сотрудников предприятия работающих со сведениями, представляющими коммерческую тайну и их ответственность за ее разглашение

1. Сотрудники предприятия, допущенные к сведениям, составляющим коммерческую тайну, несут ответственность за точное выполнение требований, предъявляемых к ним в целях обеспечения сохранности указанных сведений.

До получения доступа к работе, связанной с коммерческой тайной, им необходимо изучить настоящую инструкцию и дать в службе информационной безопасности письменное обязательство о сохранении коммерческой тайны.

2. Сотрудники предприятия, допущенные к коммерческой тайне должны:

- строго хранить коммерческую тайну. О ставших им известной утечке сведений, составляющих коммерческую тайну, а также об утрате документов с грифом «КТ», сообщать непосредственному руководителю и в службу информационной безопасности;

- предъявлять для проверки по требованию представителей службы информационной безопасности все числящиеся документы с грифом «КТ», а в случае нарушения установленных правил работы с ними представлять соответствующие объяснения;

- знакомиться только с теми документами и выполнять только те работы, к которым они допущены;

- строго соблюдать правила пользования документами, имеющими гриф «КТ». Не допускать их необоснованной рассылки;

- все полученные в делопроизводстве службы информационной безопасности или у ее уполномоченного документы с указанным грифом немедленно вносить во внутреннюю опись документов, в которой отводится специальный раздел по учету «КТ»;

- исполненные входящие документы, а также документы, предназначенные для рассылки, подшивки в дело или уничтожения сдавать в делопроизводство службы информационной безопасности или уполномоченному службы информационной безопасности;

- выполнять требования внутри объектного режима: исключающие возможность ознакомления с документами «КТ» посторонних лиц, включая и своих сотрудников, не имеющих к указанным документам прямого отношения;

- при ведении деловых переговоров с представителями сторонних организаций или частными лицами ограничиваться выдачей минимальной информации, действительно необходимой для их успешного завершения;

- исключить использование ставшей известной коммерческой тайны предприятия в свою личную пользу, а также деятельность, которая может быть использована конкурентами в ущерб предприятию – владельцу данной коммерческой тайны.

3. Ответственность за разглашение сведений, составляющих коммерческую тайну предприятия, и утрату документов или изделий, содержащих такие сведения, устанавливается в соответствии с действующим законодательством.

При этом подразумевается:

1. Под разглашением сведений, составляющих коммерческую тайну – предание огласке сведений лицом, которому эти сведения были доверены по службе, работе или стали известны иным путем, в результате чего они стали достоянием посторонних лиц.

2. Под утратой документов или изделий (предметов), содержащих сведения, относящиеся к коммерческой тайне, – выход (в том числе и временный) документов или изделий из владения ответственного за их сохранность лица, которому они были доверены по службе или работе, являющийся результатом нарушения установленных правил обращения с ними, вследствие чего эти документы или изделия стали либо могли стать достоянием посторонних лиц.