ОРЕНБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УФИМСКИЙ ФИЛИАЛ

# Контрольная работа №1

По дисциплине: «Документоведение»

Технология защиты документной информации

Студента:

Группа: ЭП 4-4

Шифр студента: 557

Учебный год: 2008-2009

Содержание

Введение

1. Работа с документами, содержащими коммерческую тайну

2. Общие методы обеспечения информационной безопасности

3. Способы и средства защиты информации

Заключение

Список использованной литературы

Введение

В эпоху глобализации, IT-технологий, когда на людей обрушиваются потоки информации, - мало знать общеизвестное; предпочтение отдаётся тому человеку, который владеет ограниченной либо недоступной для общего пользования информацией.

Одновременно с этим, что вполне закономерно, на первый план выходит необходимость защиты конфиденциальной информации, особенно это касается государственных и силовых структур, различных предприятий и организаций. В условиях жесткой конкуренции очень важно сохранять сведения, содержащие коммерческую тайну предприятия. Так как коммерческой и/или служебной тайной могут воспользоваться, преследуя корыстные цели, её следует охранять, не допуская ни малейшей утечки информации, со всей строгостью наказывая правонарушителей. Законодательство РФ регламентирует отношения в области обеспечения информационной безопасности. Основами ГК РФ введена защита конфиденциальной информации. При этом строго определено, что и при каких условиях необходимо считать коммерческой тайной, каких виды она принимает и что включает в себя.

Существуют различные виды обеспечения конфиденциальности информации. Требуются определённые условия для обеспечения конфиденциальности: определение сведений, составляющих коммерческую тайну предприятия и обеспечение порядка их защиты. Если эти правила не соблюдены, руководитель не вправе привлекать к ответственности своих сотрудников.

Менеджеры, чью прямую обязанность составляет работа с документами (понятие «документ» включает в себя информацию, адресованную/полученную любыми физическим и юридическим лицами для использования своей деятельности), должны осознавать возложенную на них ответственность и не разглашать сведений, которые составляют или только потенциально могут составлять коммерческую и служебную тайны. Сотруднику следует защищать информацию не только своей организации, но и «чужие» тайны, т.е. тайны, которую доверили организации клиенты, посредники, представители и партнёры, причём даже после увольнения эта обязанность сохраняется.

В данной контрольной большое внимание уделяется защите документации, содержащей коммерческую и/или служебную тайну. В частности, указывается порядок регистрации документов, содержащих конфиденциальную информацию; порядок напечатания, размножения и уничтожения копий и вариантов; порядок ведения, учёта, содержания, оформления, а также хранения; порядок проверки специальной комиссией; порядок распределения документов с грифом «Коммерческая тайна», их уничтожения – при присутствии должностного лица.

1. Работа с документами, содержащими коммерческую тайну

Коммерческая тайна – производственная, научно–техническая, управленческая, финансовая и иная документированная информация, используемая для достижения коммерческих целей (получения прибыли, предотвращение ущерба, получение добросовестного преимущества над конкурентами), которую предприниматель считает конфиденциальной. К конфиденциальным сведениям относятся, прежде всего идеи, изобретения, открытия, технологии, индивидуальные детали коммерческой деятельности, позволяющие успешно конкурировать, прибыль фирмы и т. п.

Основами ГК РФ введена защита технической, организационной и коммерческой информации, составляющей секреты производства («ноу-хау»). При этом установлен один общий признак – «коммерческий признак», т.е. способность быть объектом рыночного оборота. К нему относятся любые знания, включая практический опыт специалистов во всех сферах хозяйственной деятельности.

Условия, при которых информация предприятия может быть отнесена к коммерческой тайне, перечислены в статье 139 части Гражданского Кодекса РФ. К ним относятся:

* Действительная или потенциальная коммерческая деятельность информации в силу неизвестности ее третьим лицам;
* Отсутствие свободного доступа к этой информации на законном основании;
* Принятие обладателем информации необходимых мер к охране ее конфиденциальности.
* Обеспечение сохранности конфиденциальной информации коммерческого предприятия требует соблюдения следующих условий:
* Определение сведений, составляющих коммерческую тайну предприятия;
* Обеспечения порядка их защиты.

Если эти условия не будут выполнены, то у предприятия не будет законных оснований для привлечения к ответственности работников за разглашение или передачу сведений, составляющих коммерческую тайну.

Сведения коммерческой тайны предприятия можно условно разделить на два крупных блока:

* Научно – техническая (технологическая) информация;
* Деловая информация.

Научно – техническая информация включает: сведения о конструкциях машин и оборудования; чертежи; схемы; используемые материалы; рецептуры; методы и способы производства (особенно о вновь разрабатываемых изделиях); новые технологии, направления модернизации известных технологий, процессов и оборудования; программное обеспечение ПВЭМ.

Деловая информация включает:

* Сведения о финансовой стороне деятельности предприятия, за исключением финансовых отчетов (состояние расчетов с клиентами, задолженность, кредиты и т.п.);
* Сведения о размере прибыли, себестоимости произведенной продукции и др.;
* Планы развития предприятия (тактические и стратегические);
* Планы и объемы реализации продукции (планы маркетинга, данные о характере и объеме торговых операций, уровня цен, наличие товаров);
* Анализ конкурентоспособности производимой продукции, эффективность экспорта и импорта, предполагаемое время выхода на рынок;
* Планы рекламной деятельности, списки торговых и других клиентов, представителей, посредников, конкурентов, сведения о взаимоотношениях с ними, их финансовом положении, проводимых операциях и объемах, условиях действующих и заключаемых контрактов и др.

Состав и объем сведений, составляющих коммерческую тайну предприятия, сроки конфиденциальности, порядок защиты и доступа к конфиденциальной информации, а также правила ее использования определяются руководителем. Руководитель может привлечь для проведения этой работы специалистов – аналитиков.

Органы государственной власти и местного самоуправления не вправе вмешиваться в определение и охрану коммерческой тайны предприятия, за исключением случаев, предусмотренных законом.

Основная цель защиты конфиденциальной информации состоит в том, чтобы, как говорят профессионалы, предотвратить ее утечку, овладение ее конкурентами. В ряде случаев требуется защита и «чужих» коммерческих секретов, которые могут быть доверены предприятию другими лицами, организациями. Отсутствие такой защиты может лишить предприятие выгодных партнеров, клиентов.

Обеспечение защиты включает в себя:

* Установление правил отнесения информации к коммерческой тайне;
* Разработку и доведение до лиц, допущенных к сведениям, составляющим коммерческую тайну, инструкций по соблюдению режима конфиденциальности;
* Ограничение доступа к носителям информации, содержащим коммерческую тайну;
* Ведение делопроизводства, обеспечивающего выделение, учет и сохранность документов, содержащих коммерческую тайну;
* Использование организационных, технических и иных средств защиты конфиденциальной информации;
* Осуществление контроля за соблюдением установленного режима охраны коммерческой тайны.

Для ограничения доступа к информации коммерческой тайны руководитель издает специальный приказ о введении «Перечня сведений, содержащих коммерческую тайну предприятия», мер по охране этих сведений, установлению круга лиц, имеющих доступ к этой информации, и правил работы с документами, имеющими гриф «Коммерческая тайна». Сотрудники предприятия должны под расписку ознакомиться с приказом и приложениями к нему.

«Примерный перечень сведений, составляющих коммерческую тайну предприятия» приведен на рисунке 1.

В случае необходимости этот список может быть продолжен и также заверен подписью руководителя с проставлением новой даты.

Если сведения из «Перечня …» переносятся в документы, то документы становятся конфиденциальными, и от того, как будет организована работа с ними, зависит успешная деятельность предприятия.

Ведение делопроизводства, обеспечивающего учет и сохранность документов, содержащих коммерческую тайну, предусматривает выполнение ряда рекомендаций.

Приказом руководителя предприятия назначается должностное лицо (лица), ответственное за учет, хранение и использование документов, содержащих конфиденциальные сведения. Это может быть сотрудник, доля которого работа с документами, содержащими коммерческую тайну, является основной служебной обязанностью, или секретарь – референт предприятия, для которого эти функции будут дополнительными.

Все документы, содержащие конфиденциальные сведения, подлежат учету и специальному обозначению. На документе проставляют гриф конфиденциальности в правом верхнем углу первого листа с указанием номера экземпляра, например:

КТ

Экз. №1

или

Конфиденциально

Экз. №1

Такие грифы не являются грифами секретности, а лишь показывают, что право собственности на информацию, содержащуюся в документе, принадлежит предприятию и охраняется законодательно.

В тексте документа также может быть оговорена конфиденциальность сведений, права предприятия на них, порядок их использования и т.п. Например, если коммерческая тайна является результатом совместной деятельности с другим предприятием, то необходимость ее сохранения должна быть отражена в контракте. В случае отсутствия грифа «Коммерческая тайна» и указаний на конфиденциальность в тексте предполагается, что автор и лица, подписавшие или утвердившие документ, предусмотрели все возможные последствия от свободной (без ограничения доступа) работы с документом.

|  |
| --- |
| Приложениек приказу директора ЗАОот 00.00.00 №ПЕРЕЧЕНЬ СВЕДЕНИЙ,составляющих КОММЕРЧЕСКУЮ ТАЙНУЗАО «Интегра»Размер кредитов, которые взяла или собирается взять фирмаОбъем производства продукции (в месяц, квартал, год)Наименование фирм – контрагентовРазмер прибыли, получаемой за месяц, квартал, годРаспределение прибылиЦели, задачи и тактика переговоров с деловыми партнерамиУсловия коммерческих контрактов, платежей, услугСтепень заинтересованности в приобретении товара или услугЗаработная плата сотрудников предприятияХарактер и репутация персонала предприятияРегионы сбыта продукцииНаправление маркетинговых исследований предприятияДиректор подпись В.И. Завьялов |

Рисунок 1

На документе с грифом «Коммерческая тайна» («Конфиденциально») указывается количество экземпляров документа и место нахождения каждого из них (ниже реквизитов «подпись» и фамилия исполнителя»), например:

Составлен в двух экз.:

экз. №1 – а адрес;

экз. №2 – в дело № 01-07.

На обороте листа документа, имеющего гриф «Коммерческая тайна», руководитель пишет фамилии тех должностных лиц, которым разрешено пользоваться этим документом, например:

Разрешаю:

1. Лаврову Е.М.

2. Казакову А.Л.

Подпись руководителя

Дата

Печатание документов с грифом «Коммерческая тайна» производится централизованно, в специально отведенном помещении (рабочем месте), исключающим доступ посторонних лиц.

Отпечатанные и подписанные документы передаются для регистрации должностному лицу, ответственному за их учет.

Черновики и варианты документа уничтожаются этим лицом с подтверждением факта уничтожения записью на копии исходящего документа: «Черновик (и варианты) уничтожены. Подпись. Дата».

Все документы, содержащие конфиденциальную информацию, должны регистрироваться отдельно от остальной документации в «Журнале регистрации документов с грифом «Коммерческая тайна» (см. таблицу № 2. При значительном объеме документов могут быть заведены журналы отдельно для входящих, исходящих и внутренних документов предприятия, содержащих гриф «Коммерческая тайна». Все листы журналов, учитывающих документы «Коммерческая тайна», нумеруются, прошиваются и опечатываются. В конце журнала в заверительном листе указывается количество листов (цифрами и прописью).

Таблица №2 «Журнал регистрации документов с грифом «Коммерческая тайна»

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Номер(индекс)документа | Датарегист-рациидоку-мента | Дата ииндексдокумента(длявходящих) | Откудапоступилили куданаправ-лен | Краткое содержа-ние (заголовок) | Кол-во лис-тов | Кол-во экзем-пляров | Испол-нитель | Приме-чание |
|  |  |  |  |  |  |  |  |  |

Все поступающие (входящие) документы с грифом «Коммерческая тайна» принимаются и вскрываются специально назначенным должностным лицом или секретарем – референтом, если ему предоставлено такое право. При поступлении обязательно проверяется целостность корреспонденции, количество листов и экземпляров основного документа и приложений к нему. В случае отсутствия или недостачи в конвертах (пакетах) документов с грифом «Коммерческая тайна» составляется акт в двух экземплярах, один из которых направляется отправителю.

Документы, имеющие гриф «Коммерческая тайна», формируются в отдельное дело (или дела). На обложке дела в правом верхнем углу ставится гриф «Коммерческая тайна». На внутренней обложке дела пишется список сотрудников, имеющих право пользования этим делом. Все листы дела нумеруются простым карандашом в правом верхнем углу. Вначале дела подшивается внутренняя опись, содержащихся в нем, в конце дела подшивается заверительный лист. Хранятся такие дела в сейфе, который опечатывается должностным лицом, ответственным за сохранность документов с грифом «Коммерческая тайна». Другие работники предприятия не должны иметь доступ к этому сейфу.

Движение (выдача и возврат) документов с грифом «Коммерческая тайна» должно своевременно отражаться в «Журнале учета выдачи документов с грифом «Коммерческая тайна» (см. таблицу № 3).

При выдаче документа секретарем – референтом работник, получивший документ с грифом «Коммерческая тайна», должен сверить № (индекс) полученного документа с № (индексом) в журнале, проверить количество листов и поставить в журнале свою подпись.

Выданные для работы документы с грифом «Коммерческая тайна» подлежат возврату секретарю – референту в тот же день. С разрешения руководства предприятия отдельные документы с грифом «Коммерческая тайна» могут находится у исполнителя в течении срока, необходимого для выполнения работы с ними, при условии полного обеспечения сохранности документов на рабочем месте исполнителя (наличие сейфа, кодового замка и т.д.).

При возврате документов с грифом «Коммерческая тайна» секретарь – референт сверяет № документа по журналу, проверяет количество листов документа и в присутствии работника ставит в графе «Отметка о возврате» свою подпись и дату возврата документа.

Таблица № 3 «Журнал учета выдачи документов с грифом «Коммерческая тайна»

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Индексдоку-мента | Датавыда-чи | Краткоесодержание(заголовок) | Кол-во экз. | Кол-во листов | Комувыдано(Ф.И.О.) | Подписьза полу-ченныйдокумент | Отметка о возврате(подпись и дата) | Приме-чание |
|  |  |  |  |  |  |  |  |  |

Передача документов и дел другим работникам предприятия, имеющим допуск к этим документам, производится только через секретаря – референта с обязательной записью в журнале.

Запрещается изъятие из дел или перемещение документов с грифом «Коммерческая тайна» из одного дела в другое без разрешения руководства отметок в «Журнале регистрации документов с грифом «Коммерческая тайна».

Документы с грифом «Коммерческая тайна» запрещается выносить из офиса. Лишь в исключительных случаях руководитель или его заместители могут разрешить сотрудникам вынос таких документов из здания для согласования, подписания и т.п. с принятием необходимых мер предосторожности.

На предприятии должен быть принят строгий порядок размножения документов с грифом «Коммерческая тайна». Они должны копироваться с разрешения руководства предприятия в специально выделенном помещении. Все копии документов, составляющие «Коммерческую тайну» берутся на учет в специальном журнале или в «Журнале регистрации документов с грифом «Коммерческая тайна» количество экземпляров документов с грифом «Коммерческая тайна» должно быть ограниченно, причем каждый экземпляр готовится для заранее определенного адресата или исполнителя. Размножение документов следует производить в присутствии должностного лица, ответственного за документ. Все бракованные копии документа им забираются и подлежат немедленному уничтожению.

Все дела с грифом «Коммерческая тайна», журналы (картотеки) учета документов, содержащих «Коммерческую тайну» в обязательном порядке вносятся в номенклатуру дел предприятия.

По окончании года специально созданная комиссия предприятия выполняет следующие работы:

* Проверяет наличие всех документов с грифом «Коммерческая тайна»;
* Отбирает документы с грифом «Коммерческая тайна» для архивного хранения;
* Отбирает документы с грифом «Коммерческая тайна» для уничтожения.

Проверка наличия документов с грифом «Коммерческая тайна» по разрешению руководства предприятия может производится с другой периодичностью, например, по окончании каждого квартала.

В случае установления факта утраты документом с грифом «Коммерческая тайна» немедленно ставится в известность руководитель предприятия, и принимаются все меры по розыску документа. Для расследования факта утраты руководителем предприятия назначается комиссия.

На утерянные документы после того, как розыск их не принес положительных результатов, составляется акт. В «Журнале регистрации документов с грифом «Коммерческая тайна» вносятся соответствующие отметки об утрате.

При увольнении сотрудника, ответственного за документы с грифом «Коммерческая тайна», производится проверка числящихся за ним документов и их передача вновь назначенному лицу.

Акт приема – передачи этих документов утверждается руководителем предприятия или его заместителем.

При прекращении трудовых отношений с предприятием, на котором сотрудник был допущен к «Коммерческой тайне», обязательства о неразглашении конфиденциальных сведений действуют в течение двух лет, если иной срок не установлен трудовым контрактом.

При передаче дел в архив на документы с грифом «Коммерческая тайна» составляется отдельная опись.

Архивное хранение таких документов производится в опечатанных коробках, в помещениях, исключающих несанкционированный доступ.

На документах с грифом «Коммерческая тайна», отобранные к уничтожению, составляется акт, утверждаемый руководителем предприятия.

Уничтожаются документы в присутствии комиссии с помощью специальной машины или иным способом, исключающим возможность восстановления имеющейся в ней информации.

2. Общие методы обеспечения информационной безопасности

Общие методы обеспечения информационной безопасности подразделяются на правовые, организационно – технические и экономические.

К правовым методам обеспечения информационной безопасности относится разработка нормативных правовых актов, регламентирующих отношения в информационной сфере, и нормативных методических документов по вопросам обеспечения информационной безопасности. Наиболее важными направлениями этой деятельности является:

* внесение изменений и дополнений в законодательство РФ, регламентирующее отношения в области обеспечения информационной безопасности в целях создания и совершенствования системы обеспечения информационной безопасности, устранение внутренних противоречий в федеральном законодательстве, противоречий, связанных с международными соглашениями, к которым присоединяется РФ, и противоречий между федеральными законодательными актами и законодательными актами всех субъектов РФ, а также в целях конкретизации правовых норм, устанавливающих ответственность за правонарушения в области обеспечения информационной безопасности;
* законодательное разграничение полномочий в области обеспечения информационной безопасности РФ между федеральными органами государственной власти и органами государственной власти субъектов РФ, определение целей, задач и механизмов участия в этой деятельности общественных объединений, организаций и граждан;
* разработка и принятие нормативных правовых актов РФ, устанавливающих юридических и физических лиц за несанкционированный доступ к информации, ее противоправное копирование, искажение и противозаконное использование, преднамеренное распространение недостоверной информации, противоправное раскрытие конфиденциальной информации, использование в преступных и корыстных целях служебной информации или информации, содержащей коммерческую тайну;
* уточнение статуса иностранных информационных агентств, средств массовой информации и журналистов, а также инвесторов при привлечении иностранных инвестиций для развития иностранной инфраструктуры России;
* законодательное закрепление приоритета развития национальных сетей связи и отечественное производство космической, спутниковой связи;
* определение статуса организаций, предоставляющих услуги глобальных информационно – телекоммуникационных сетей на территории РФ, и правовое регулирование деятельности этих организаций;
* создание правовой базы для формирования в РФ региональных структур обеспечения информационной безопасности.

Организационно – техническими методами обеспечения являются:

* Создание и совершенствование системы обеспечения информационной безопасности РФ;
* Усиление правоприменительной деятельности федеральных органов исполнительной власти субъектов РФ, включая предупреждение и пресечение правонарушений в информационной сфере, а также выявление, изобличение и привлечение к ответственности лиц, совершивших преступления и другие правонарушения в этой сфере;
* Разработка, использование и совершенствование средств защиты процессов переработки информации и методов контроля эффективности этих средств, развитие защищенности телекоммуникационных систем, повышение надежности специального программного обеспечения;
* Создание систем и средств, предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушения, уничтожение, искажение информации, а также изменение штатных режимов функционирования систем информатизации и связи;
* Выявление технических устройств и программ предоставляющих опасность для нормального функционирования информационно – телекоммуникационных систем, предотвращение перехвата информации по техническим каналам, применение криптографических средств защиты процессов переработки информации при ее хранении, обработке и передаче по каналам связи, контроль за выполнением специальных требований по защите;
* Сертификация средств защиты процессов переработки информации, лицензирование деятельности в области защиты государственной тайны, стандартизация способов и средств защиты;
* Совершенствование системы сертификации телекоммуникационного оборудования и программного обеспечения автоматизированных систем обработки информации по требованию информационной безопасности;
* Контроль за действиями персонала в защищенных информационных системах, подготовка кадров в области обеспечения информационной безопасности РФ;
* Формирование системы мониторинга показателей и характеристик информационной безопасности РФ и наиболее важных сферах жизни и деятельности общества и государства.

Экономические методы, обеспечивающие ИБ РФ включают в себя:

* разработку программ, обеспечивающих ИБ РФ и определяющих порядок их функционирования;
* совершенствование системы финансирования работ, связанных с реализацией правовых и организационно-технических методов защиты процессов переработки информации, создание системы страхования информационных рисков физических и юридических лиц.
* Следовательно, именно на этих этапах должны быть сосредоточены основные усилия при создании защищённых систем.

3. Способы и средства защиты информации

Необходимость обеспечения скрытности (секретности) отдельных замыслов, действий, сообщений возникла в глубокой древности, практически вместе с началом осмысленной человеческой деятельности. Иначе говоря, организация защиты части информации от несанкционированного доступа к ней – проблема столь же древняя, как и само понятие «информация».

На современном этапе существуют следующие предпосылки сложившейся кризисной ситуации обеспечения безопасности информационных систем (ИС):

* современные компьютеры за последние годы приобрели большую вычислительную мощность, но одновременно с этим стали проще в эксплуатации;
* прогресс в области аппаратных средств сочетается с ещё большим развитием программного обеспечения;
* развитие гибких и мобильных технологий обработки информаций привело к тому. Что практически исчезает грань между обрабатываемыми данными и исполняемыми программами за счёт появления и широкого распространения виртуальных машин и интерпретаторов;
* несоответствие бурного развития средств обработки информации и медленной проработки теории информационной безопасности привело к появлению существенного разрыва между теоретическими моделями безопасности, оперирующими абстрактными понятиями типа «объект», «субъект» и реальными категориями современных ИТ;
* необходимость создания глобального информационного пространства и обеспечение безопасности протекающих в нём процессов потребовали разработки международных программ и стандартов, следование которым может обеспечить необходимый уровень гарантии обеспечения защиты.

Вследствие совокупного действия всех перечисленных факторов перед разработчиками современных ИС, предназначенных для обработки конфиденциальной информации, стоят следующие задачи, требующие немедленного и эффективного решения:

* обеспечение безопасности новых типов информационных ресурсов;
* организация доверенного взаимодействия сторон (взаимной идентификации (аутентификации) в информационном пространстве;
* защита от автоматических средств нападения;
* интеграция в качестве обязательного элемента защиты информации в процессе автоматизации её обработки.

В настоящее время с ростом объёмов обработки информации в компьютерных сетях, расширением круга её потребителей, распространением многопрограммных режимов работы ЭВМ, внедрением перспективных ИТ данная проблема приобрела новый аспект в связи с возрастанием роли программно-технического посредника между человеком-пользователем и информационными объектами, что, в свою очередь, вызвало создание дополнительных способов закрытия информации.

Понятно, что проблема защиты информации приобретает особое значение в экономической области, характеризующейся повышенными требованиями одновременно к скрытности и оперативности обработки информации.

Учитывая наибольшую сложность обеспечения защиты информации, обрабатываемой и передаваемой в компьютерных сетях различных типов, в дальнейшем рассматривается, прежде всего, эта часть проблемы (если иное не оговаривается специально).

Анализ уязвимости машинной информации позволяет выделить две группы возможных причин её искажения или уничтожения:

* непреднамеренные действия (сбои технических средств, ошибки обслуживающего персонала, аварии и т.п.);
* несанкционированные действия, к которым относятся: НСД и ознакомление субъектов с информацией;
* прямое хищение информации электронном виде непосредственно на носителях или копирование информации на другие носители;
* запрещённая передача информации в линии связи или на терминалы; перехват электромагнитных излучений и информации по различным каналам связи и т.п.

Такое большое количество причин искажения и уничтожения информации определяет необходимость использования и значительного числа способов и средств её защиты, причём эти способы и средства эффективны только тогда, когда применяются комплексно. Названные обстоятельства обуславливают содержание понятия «защита электронной информации».

Под защитой информации в компьютерных системах понимают создание и поддержание организованной совокупности средств, способов, методов и мероприятий, предназначенных для предупреждения искажения, уничтожения и несанкционированного использования информации, хранимой и обрабатываемой в электронном виде.

Наряду с определением понятия «защита информации» важным вопросом является классификация имеющихся способов и средств защиты, которые позволяют воспрепятствовать несанкционированному использованию. На рис.2 Приведены наиболее часто используемые способы защиты информации, которыми они могут быть реализованы (эти возможности изображены стрелками от способа к средствам).

Побуждение

Морально-этические

Законодательные

Принуждение

Организационные

Регламентация

Способы

Универсальные

Средства

Маскировка

Специализированные

Управление доступом оододоступом

Технические

Аппаратные

Препятствия

Физические

Рисунок 2. Способы и средства защиты информации.

Рассмотрим каждый из способов. Препятствия предусматривают создание преград, физически не допускающих к информации. Управление доступом – способ защиты информации за счёт регулирования использования всех ресурсов системы (технических, программных и др.).

Маскировка информации, как правило, осуществляется путём её криптографического закрытия. Регламентация заключается в реализации системы организационных мероприятий, определяющих все стороны обработки информации. Принуждение заставляет соблюдать определённые правила работы с информацией под угрозой материальной, административно уголовной ответственности. Наконец, побуждение основано на использование действенности морально-этических категорий (например, авторитета или коллективной ответственности).

Средства защиты информации, хранимой и обрабатываемой в электронном виде, разделяют на три самостоятельные группы: технические, программные и социально-правовые. В свою очередь, среди технических средств выделяют физические и аппаратные.

К физическим средствам защиты относятся:

* механические преграды, турникеты, специальное остекление;
* сейфы, шкафы;
* механические и электромеханические замки, в том числе и с дистанционным управлением;
* замки с кодовым набором;
* датчики различного типа;
* теле - и фотосистемы наблюдения и регистрации;
* СВЧ, ультразвуковые, радиолокационные, лазерные, акустические системы и др.;
* устройства маркировки;
* устройства с идентификационными картами;
* устройства идентификации по физическим признакам;
* устройства пространственного заземления;
* системы физического контроля доступа;
* системы охранного телевидения и охранной сигнализации;
* системы пожаротушения и оповещения о пожаре и др.

Под аппаратными средствами защиты понимают технические устройства, встраиваемые непосредственно в системы (аппаратуру) обработки информации. Наиболее часто используют:

* регистры хранения реквизитов защиты (паролей, грифов секретности и др.);
* устройства для измерения индивидуальных характеристик человека (цвет и строение радужной оболочки глаз, овала лица и др.);
* схемы контроля границ адреса имён для определения законности обращения к соответствующим областям памяти и отдельным программам;
* схемы прерывания передачи информации в линии связи с целью периодического контроля адресов выдачи данных);
* экранирование ЭВМ;
* установка генераторов помех и др.

Программные средства защиты данных в настоящее время получили значительное развитие. По целевому назначению их можно разделить на несколько больших групп:

* программы идентификации пользователей;
* программы определения прав (полномочий) пользователей (технических устройств);
* программы регистрации работы технических средств и пользователей (ведение так называемого технического журнала);
* программы уничтожения (затирания) информации после решения соответствующих задач или при нарушении пользователем определённых правил обработки информации;
* Криптографические программы (программы шифрования данных).

Программные средства защиты информации делятся на средства, реализуемые в стандартных ОС (универсальные), и программные средства защиты в специализированных ИС (специализированные). К первой группе относятся:

* динамическое распределение ресурсов и запрещение задачам пользователей работать с чужими ресурсами;
* разграничение доступа пользователей к ресурсам по паролям;
* разграничение доступа пользователей к информации по ключам защиты;
* защита таблицы паролей с помощью главного пароля и др.

Средства защиты в экономических ИС, в том числе банковских системах, позволяют реализовать следующие функции защиты данных:

* опознавание по идентифицирующей информации пользователей и элементов ИС, разрешение на этой основе работы с информацией на определённом уровне;
* ведение многоразмерных таблиц профилей доступа пользователей к данным;
* управление доступом по профилям полномочий;
* уничтожение временно фиксируемых областей информации при завершении её обработки;
* формирование протоколов обращения к защищаемым данным с идентификацией данных о пользователе и временных характеристик;
* программная поддержка работы терминала лица, отвечающего за безопасность информации;
* подача сигналов при нарушении правил работы с системой или правил обработки информации;
* физическая или программная блокировка возможности работы пользователя при нарушении им определённой последовательности правил или совершения определённых действий;
* подготовка отчётов о работе с различными данными – ведение подробных протоколов работы и т.п.;

Криптографические программы основаны на использовании методов кодировки (оцифровки) информации. Данные методы остаются достаточно надёжными средствами её защиты.

В перспективе можно ожидать развития программных средств защиты по двум основным направлениям:

* создание централизованного ядра безопасности, управляющего всеми средствами защиты информации в ЭВМ (на первом этапе – в составе ОС, затем – вне её);
* децентрализация защиты информации вплоть до создания отдельных средств, управляемых непосредственно только пользователем. В рамках этого направления находят широкое применение методы «эстафетной палочки» и «паспорта», основанные на предварительном расчёте специальных контрольных кодов (по участкам контролируемых программ) и их сравнении с кодами, получаемыми в ходе решения задачи.

Организационные и законодательные средства защиты информации предусматривают создание системы нормативно-правовых документов, регламентирующих порядок разработки, внедрения и эксплуатации информации, а также ответственность должностных и юридических лиц за нарушение установленных правил, законов, стандартов и т.п.

Морально-этические средства защиты информации основаны на использовании моральных и этических норм, принятых в обществе, и требуют от руководителей всех рангов особой заботы о создании в коллективах здоровой нравственной атмосферы.

Заключение

Таким образом, мы наблюдаем, что, в связи с постепенным переходом на новый этап развития (постиндустриальная эпоха), информация становится ключевой фигурой, управляющей жизнедеятельностью различных групп и сообществ. Условно говоря, из объекта деятельности начинает становиться субъектом. Трудно представить себе профессию, не использующую в своей деятельности информацию; для менеджеров же – это профессиональный продукт, благодаря которой осуществляются управление и организация системами производства.

Технология защиты документации, обеспечение защиты конфиденциальной информации всеми возможными и допустимыми средствами – есть необходимое и наиважнейшее условие. В экономической области, характеризующейся повышенными требованиями к секретности и, в тоже время, оперативности обработки информации, проблема защиты информации приобретает особое значение. Как уже было оговорено ранее, существует особый порядок защиты документации, созданы разнообразные средства (законодательные, физические, аппаратные, программные, организационные, морально-этические) и методы защиты (правовые, организационно-технические, экономические). Таким образом обеспечивается контроль работы с организационно-распорядительными документами. Базовый процесс всех управленческих функций подлежит чёткой и понятной организации, где источник утечки информации легче выявить.

Приходим к выводу, что технология защиты документной информации является необходимым условием слаженной и безопасной деятельности предприятий и организаций.

Список использованной литературы

1. Борискин В.В. Официальное делопроизводство: виды и формы документов: учебно – практическое пособие – 2-е изд., - М.: Омега – Л, 2006. – 197.
2. Демин М.Ю. Делопроизводство. Документный менеджмент. – М.: 2004. – 197.
3. Мельников В.П. Информационная безопасность. Учебное пособие. М.: Издательский центр, «Академия», 2005. 336.
4. Румынина Л.А. Делопроизводство. М.: Мастерство, 2002. – 208.
5. Стенюков М.В. Документы. Делопроизводство. – М. «ПРИОР», 2000. 144.
6. Сотов П.В. Тихомиров А.Н. Делопроизводство. Образцы документов, инструкции, ГОСТы. – М.: Проспект, 2001. – 80.
7. Чуковенков А.Ю. Янковская В.Ф. Оформление документов. Комментарий к ГОСТу 6.30 -97, Унифицированная система документации. Серия «Управление документацией». Учебно – методический центр документоведения и управления научно внедренческой фирмой «Межрегионсервис». – М.: Дело, 1999. – 232.