65.050.2 я 73
М 545
№ 2780 - 2

МИНИСТЕРСТВО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ТАГАНРОГСКИЙ ГОСУДАРСТВЕННЫЙ РАДИОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

Кафедра Безопасности информационных технологий

Методическое пособие
Основы защищенного делопроизводства
по курсу
Технология защищенного документооборота

Часть 2

Для студентов специальностей 075300, 075400, 075500

ФИБ

Таганрог 2000 г.

ББК: 65.050.2 я 73

Составители: О.Б. Макаревич, Л.К. Бабенко, А.К. Шилов, А.В. Коваленко.

Методическое пособие «Основы защищенного делопроизводства» по курсу «Технология защищенного документооборота». Таганрог: Изд-во ТРТУ, 2000. 79 с.

Пособие составлено на основе практического опыта государственных и коммерческих предприятий с учетом действующих нормативно-методических документов Российской Федерации.

Содержит материал по двум неразрывно связанным компонентам делопроизводства:

- организация работы с документами под грифом «Коммерческая тайна»
- составление документов под грифом «Коммерческая тайна» и правила их оформления.

Требования к оформлению документов даны на основе стандарта ГОСТ Р 6.30-97, введенного в действие с 1 июля 1998 года.

Ил. 4. Библиогр: 16 назв.

Рецензент М.В. Новиков, канд. эконом. наук, доцент кафедры ГиМУ ТРТУ.

1. МЕТОДОЛОГИЯ ФОРМИРОВАНИЯ ТРЕБОВАНИЙ К СИСТЕМЕ ЗАЩИЩЕННОГО ДОКУМЕНТООБОРОТА

Обоснование требований к защите информации является первоочередной и основополагающей задачей проектирования систем защищенного документооборота, поскольку результаты ее решения составляют исходную базу для решения всех последующих задач при всех вариантах проектирования. В то же время формальные методы объективного обоснования требований отсутствуют и возможности их разработки более чем проблематичны. Поэтому задача обоснования требований неизбежно будет решаться неформальными методами, а для повышения полноты и объективности решения целесообразно заблаговременно разработать развитую систему рекомендаций, исходя из современных возможностей и условий автоматизированной обработки информации. Рекомендации должны рассматриваться лишь в качестве первого приближения, поскольку системно-концептуальные исследования данной проблемы еще только предстоит выполнить.

Совершенно очевидно, что при обработке информации в автоматизированных системах обработки данных (АСОД) имеют силу и должны соблюдаться требования всех действующих в стране документов, регламентирующих правила обращения со сведениями, содержащими военную, государственную, промышленную, торговую или иную тайну. Кроме того, должны соблюдаться дополнительные требования, обуславливаемые спецификой автоматизированной обработки информации.

С целью целенаправленного выбора требований, при обеспечении защищенного документооборота, каждому элементу АСОД, имеющему самостоятельное территориальное размещение, должна быть определена категория по требуемой защищенности и должны соблюдаться все специальные требования, обусловливаемые категорией АСОД.

Конкретные требования к защите документооборота, обусловленные спецификой автоматизированной обработки информации, определяются совокупностью следующих факторов:

- характером обрабатываемой информации;
- объемом обрабатываемой информации;
- продолжительностью пребывания информации в АСОД;
- структурой АСОД; видом защищаемой информации;
- технологией обработки информации;
- организацией информационно-вычислительного процесса в АСОД;
- этапом жизненного цикла АСОД.

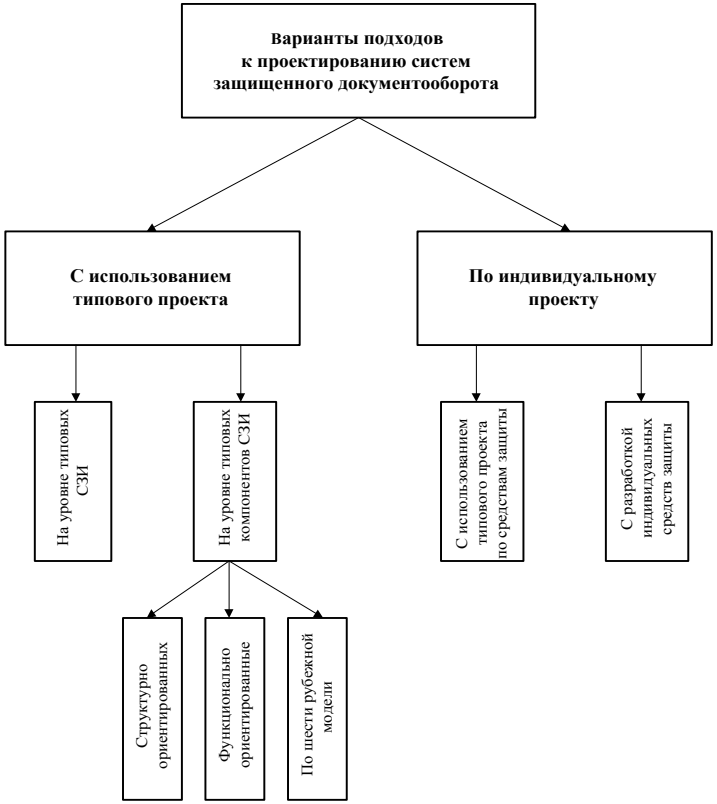

Рис. 1. Классификационная структура подходов к проектированию систем защиты информации при документообороте.

По характеру (с точки зрения требуемой защиты) информацию можно разделить на общедоступную, конфиденциальную (личную, персональную), служебную, секретную и совершенно секретно. Соответствующие рекомендации по предъявлению требований к защите могут быть следующими:

при обработке общедоступной информации никаких специальных мер защите от несанкционированного доступа не требуется;

требования к защите конфиденциальной информации определяет пользователь, устанавливающий статус конфиденциальности;

требования к защите грифованной информации определяются следующим образом:

при обработке информации с грифом «Для служебного пользования» к ней должен быть обеспечен свободный доступ пользователям учреждения-владельца этой информации; доступ же пользователей, не включенных в общий

список, должен осуществляться по разовым санкциям, выдаваемым пользователями, включенными в список;

при обработке информации с грифом «Секретно» в зависимости от ее объема и характера может быть предъявлен один из следующих вариантов требований:

1. персональное разграничение;

2. коллективное разграничение.

Требования, определяемые структурой АСОД могут быть сформулированы в следующем виде.

Информация должна защищаться во всех структурных элементах АСОД, причем специфические требования к ЗИ в структурных элементах различного типа сводятся к следующему.

В аппаратуре и линиях связи:

1. защищаемая информация должна находиться только в течение сеанса; в ЗУ аппаратуры связи могут храниться только служебные части передаваемых сообщений;

2. линии связи, по которым защищаемая информация передается в явном виде, должны находиться под непрерывным контролем во все время передачи информации;

3. перед началом каждого сеанса передачи защищаемой информации должна осуществляться проверка адреса выдачи данных;

4. при передаче большого объема защищаемой информации проверка адреса передачи должна также периодически производиться в процессе передачи (через заданный промежуток времени или после передачи заданного числа знаков сообщения);

5. при наличии в составе аппаратуры связи процессоров и ЗУ должна вестись регистрация данных о всех сеансах передачи защищаемой информации;

6. должны быть предусмотрены возможности аварийного уничтожения информации, находящейся в аппаратуре связи.

В центральном вычислителе:

1. защищаемая информация в ОЗУ может находиться только во время сеансов решения соответствующих задач, в ВЗУ - минимальное время, определяемое технологией функционирования автоматизируемых процессов;

2. и 3.— аналогично соответствующим пунктам требований к защите УГУВВ;

4. при обработке защищаемой информации должно осуществляться установление подлинности всех участвующих в обработке устройств и пользователей и ведение протоколов их работы;

5. всякое обращение к защищаемой информации должно проверяться на санкционированность;

6. при обмене защищаемой информации, осуществляемой с использованием линий связи, должна осуществляться проверка адреса корреспондента;

7. должны быть предусмотрены возможности аварийного уничтожения всей информации, находящейся в центральном вычислителе, и подачи команды на аварийное уничтожение информации в сопряженных устройствах.

В ВЗУ:

1. сменные носители информации должны находиться на устройствах управления в течение минимального времени, определяемого технологией автоматизированной обработки информации;

2. устройства управления ВЗУ, на которых установлены, носили с защищаемой информацией, должны иметь замки, предупреждающие несанкционированное изъятие или замену носителя;

3. должны быть предусмотрены возможности автономного аварийного уничтожения информации на носителях, находящихся на устройствах ВЗУ.

В хранилище носителей:

1. все носители, содержащие защищаемую информацию, должны иметь четкую и однозначную маркировку, которая, однако, не должна раскрывать содержания записанной на них информации;

2. носители, содержащие защищаемую информацию, должны храниться таким образом, чтобы исключались возможности несанкционированного доступа к ним;

3. при выдаче и приемке носителей должна осуществляться проверка личности получающего (сдающего) и его санкции на получение (сдачу) этих носителей;

4. должны быть предусмотрены возможности аварийного уничтожения информации на носителях, находящихся в хранилищах.

В устройствах подготовки данных:

1. защищаемая информация должна находиться только в течение времени ее подготовки;

2. устройства подготовки должны быть размещены так, чтобы исключались возможности просмотра обрабатываемой информации со стороны;

3. в специальных регистрационных журналах должны фиксироваться время обработки информации, исполнители, идентификаторы использованных носителей и возможно другие необходимые данные;

4. распределение работ между операторами должно быть таким, чтобы минимизировать осведомленность их о содержании обрабатываемой информации;

5. должны быть предусмотрены возможности аварийного уничтожения информации, находящейся в подразделениях подготовки данных.

Требования к защите информации, обуславливаемые территориальной распределенностью АСОД, заключаются в следующем:

в компактных АСОД (размещенных в одном помещении) достаточно организовать и обеспечить требуемый уровень защиты в пределах того помещения, в котором размещены элементы АСОД;

в слабораспределенных АСОД (размещенных в нескольких помещениях,

но на одной и той же территории) дополнительно к предыдущему должна быть обеспечена требуемая защита информации в линиях связи, с помощью которых сопрягаются элементы АСОД, расположенные в различных помещениях, для чего должны быть или постоянный контроль за этими линиями связи, или исключена передача по ним защищаемой информации в явном виде;

в сильнораспределенных АСОД (размещенных на нескольких территориях) дополнительно к предыдущему должна быть обеспечена требуемая защита информации в линиях связи большой протяженности, что может быть достигнуто предупреждением передачи по ним защищаемой информации в открытом виде.

Требования, обусловливаемые видом защищаемой информации, могут быть сформулированы в таком виде.

К защите документальной информации предъявляются следующие требования: должна обеспечиваться защита как оригиналов документов, так и сведений о них, накапливаемых и обрабатываемых в АСОД; применяемые средства и методы защиты должны выбираться с учетом необходимости обеспечения доступа пользователям различных категорий: персонала делопроизводства и библиотеки оригиналов, специалистов подразделения первичной обработки документов, специалистов функциональных подразделений автоматизируемых органов.

При обработке фактографической быстроменяющейся информации должны учитываться требования: применяемые средства и методы защиты не должны существенно влиять на оперативность обработки информации; применяемые средства и методы защиты должны выбираться с учетом обеспечения доступа к защищаемой информации строго ограниченного круга лиц.

К защите фактографической исходной информации предъявляются требования: каждому пользователю должны быть обеспечены возможности формирования требований к защите создаваемых им массивов данных в пределах предусмотренных в АСОД возможностей защиты; в системе защиты должны быть предусмотрены средства, выбираемые и используемые пользователями для защиты своих массивов по своему усмотрению.

К защите фактографической регламентной информации предъявляются требования: применяемые средства и методы должны быть рассчитаны на длительную и надежную защиту информации; должен обеспечиваться доступ (в пределах полномочий) широкого круга пользователей; повышенное значение приобретают процедуры идентификации, опознавания, проверки полномочий, регистрации обращений и контроля выдачи.

Требования, обусловливаемые технологическими схемами автоматизированной обработки информации, сводятся к тому, что в активном состоянии АСОД должна обеспечиваться защита на всех технологических участках автоматизированной обработки информации и во всех режимах.

С точки зрения организации вычислительного процесса в АСОД требуемая защита должна обеспечиваться при любом уровне автоматизации обработ-

ки информации, при всех способах взаимодействия пользователей со средствами автоматизации и при всех режимах работы комплексов средств автоматизации.

Специфические требования к защите для различных уровней автоматизации обработки информации состоят в следующем:

1. при автономном решении отдельных задач или их комплексов основными макропроцессами автоматизированной обрастай, в ходе которых должен обеспечиваться необходимый уровень защиты, являются: сбор, подготовка и ввод исходных данных, необходимых для решения задач; машинное решение задач в автономном режиме; выдача результатов решения;

2. в случае полусистемной обработки дополнительно к предыдущему на участках комплексной автоматизации должна быть обеспечена защита в ходе осуществления следующих макропроцессов: автоматизированного сбора информации от датчиков и источников информации; диалогового режима работы пользователей с ЭВМ;

3. в случае системной обработки дополнительно к предыдущему должна быть обеспечена защита в ходе таких макропроцессов: прием потока запросов и входной информации; формирование пакетов и очередей запросов; диспетчирование в ходе выполнения запросов; регулирование входного потока информации.

В зависимости от способа взаимодействия пользователей с комплексом средств автоматизации предъявляются следующие специфические требования:

при автоматизированном вводе информации должны быть обеспечены условия, исключающие несанкционированное попадание информации одного пользователя (абонента) и массив другого. Кроме того, должны быть обеспечены возможности фиксирования и документального закрепления момента передачи информации пользователя банку данных АСОД и содержания этой информации:

при неавтоматизированном вводе должна быть обеспечена защита на неавтоматизированных коммуникациях «Пользователь - ИВС», на участках подготовки (перфорации) данных и при вводе с местных УГУВВ;

при пакетном выполнении запросов пользователей должно исключаться размещение в одном и том же пакете запросов на обработку информации различных ограничительных грифов;

при обработке запросов пользователей в реальном масштабе времени данные, поступившие от пользователей, и данные, подготовленные для выдачи пользователям, в ЗУ АСОД должны группироваться с ограничительным грифом, при этом в каждой группе должен быть обеспечен уровень защиты, соответствующий ограничительному грифу данных группы:

В зависимости от режима функционирования комплексов средств автоматизации предъявляют следующие специфические требования:

в однопрограммном режиме работы в процессе выполнения программы должны предупреждаться: несанкционированное обращение к программе, не-

санкционированный ввод данных для решаемой задачи, несанкционированное прерывание выполняемой программы и несанкционированная выдача результатов решения;

в мультипрограммном режиме сформированные выше требования относятся к каждой из выполняемых программ; дополнительно к этому должно быть исключено несанкционированное использование данных одной программы другой;

в мультипроцессорном режиме сформулированные выше требования должны обеспечиваться одновременно во всех участвующих в решении задачи процессоров, кроме того, должно быть исключено несанкционированное вклинивание в вычислительный процесс при распараллеливании программ и при диспетчеризации мультипроцессорного выполнения программ.

Требования, обуславливаемые этапом жизненного цикла АСОД, формируются так:

на этапе создания АСОД должно быть обеспечено соответствие возможностей системы защиты требованиям к защите информации, сформулированным в задании на проектирование; кроме того, должно быть исключено несанкционированное включение элементов (блоков) в компоненты АСОД (особенно системы защиты);

на этапе функционирования АСОД в пассивном ее состоянии должна быть обеспечена надежная защита хранящейся информации и исключены возможности несанкционированных изменений компонентов системы;

на этапе функционирования в активном состоянии АСОД дополнительно к сформированным выше требованиям должна быть обеспечена надежная защита информации во всех режимах автоматизированной ее обработки.

Так могут быть представлены общие рекомендации по формированию требований к защите информации.

2. ДОКУМЕНТООБОРОТ И КОММЕРЧЕСКАЯ ТАЙНА

В нашей стране до недавнего времени существовало два понятия - военная и государственная тайна, что говорило о полном отсутствии логики в понятии секретности. В 1993 году парламентом принят Закон Российской Федерации «О государственной тайне». В нем наконец-то четко определено: «Государственная тайна - это защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нести ущерб безопасности Российской Федерации».

В нем законодатели разъяснили, чего не должны знать россияне: о содержании стратегических и оперативных планов, о направлениях развития вооружения и военной техники, о количестве, устройстве и технологии производства ядерного оружия, о силах и средствах гражданской обороны, о системах специальной связи и т. д.

Теперь они вправе получить сведения о чрезвычайных происшествиях и

катастрофах, о стихийных бедствиях, их официальных прогнозах и последствиях, о состоянии экологии, охраны труда, здравоохранения, санитарии, преступности, о привилегиях, компенсациях и льготах, которые предоставляет государство гражданам, должностным лицам, предприятиям и учреждениям, о фактах нарушений прав и свобод человека, о размерах золотого запаса и государственных валютных резервов, о фактах нарушения законности органами государственной власти и их должностными лицами.

В настоящее время сделан еще один шаг - разделение тайны на государственную и коммерческую. Таким образом, из области публичного права выделился институт частного права, который защищает интересы предпринимателей.

Чем отличается коммерческая тайна от государственной?

Сведения, составляющие государственную тайну, установлены соответствующим перечнем и подлежат защите со стороны государства. Коммерческая тайна перечнем не определена, поскольку она всегда разная применительно к различным предприятиям или фирмам. Другое отличие состоит в том, что государственная тайна охраняется силой государства в лице соответствующих органов, а коммерческая тайна - службой безопасности предприятия. При этом следует иметь в виду, что коммерческие секреты могут быть государственными секретами, однако государственные секреты не могут быть коммерческой тайной, поскольку в противном случае шла бы торговля государственными интересами.

В повседневной жизни коммерческая тайна всегда выступает в форме коммерческих секретов. Поэтому всякая тайна есть секрет, но не всякий секрет есть тайна. Исходя их этого попробуем дать определение коммерческой тайны и коммерческого секрета.

Коммерческая тайна - преднамеренно скрываемые по коммерческим соображениям экономические интересы и сведения о различных сторонах и сферах производственно-хозяйственной, управленческой, научно-технической, финансовой деятельности фирмы, охрана которых обусловлена интересами конкуренции и возможными угрозами экономической безопасности фирмы. Коммерческая тайна возникает тогда, когда она представляет интерес для коммерции.

Коммерческие секреты - форма проявления коммерческой тайны. Представляют собой сведения в виде документов, схем, изделий, относящиеся к коммерческой тайне фирмы и подлежащие защите со стороны службы безопасности от возможных посягательств путем похищения, выведывания, утечки информации. Они различаются по следующим признакам:

- по природе коммерческой тайны (технологические, производственные, организационные, маркетинговые, интеллектуальные, рекламные);
- по принадлежности собственнику (собственность предприятия, группы предприятий, отдельного лица, группы лиц);
- по назначению коммерческих секретов. Документы, содержащие ком-

мерческие секреты, могут иметь гриф «Конфиденциально», «Строго конфиденциально», «Конфиденциально, только адресату» и другие.

Правила засекречивания сведений, составляющих государственную тайну, утверждены Постановлением правительства России. Сведения, содержащие государственную тайну, по степени их секретности подразделяются на три категории: сведения особой важности, совершенно секретные сведения и просто секретные.

К сведениям особой важности отнесены сведения, разглашение которых нанесет ущерб интересам Российской Федерации в одной или нескольких областях: военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности.

К совершенно секретным - сведения из тех же областей, разглашение которых нанесет ущерб интересам одного ведомства или одной отрасли экономики.

К секретным - все остальные сведения, составляющие государственную тайну.

Составленные перечни секретных сведений будут доводиться до органов государственной власти, а также предприятий и организаций, имеющих дело с государственной тайной, но не целиком, а только в части, их касающейся.

Пересматриваются перечни не реже, чем раз в 5 лет, а также при изменении международной обстановки, появлении новых достижений в области науки и техники.

Носитель коммерческого секрета - лицо, осведомленное о коммерческих секретах предприятия или фирмы (руководители и допущенные к коммерческим секретам исполнители).

Носителей коммерческих секретов следует отличать от **источников закрытой коммерческой информации** («ноу-хау», схемы, документы, технологии, изделия, образцы).

Секретность в условиях рыночного хозяйствования защищает производителя от недобросовестной конкуренции, к которой относятся различные противоправные действия в виде скрытого использования торговой марки, подделки продукции конкурента, обманной рекламы, подкупа, шантажа. Не последнее место в этом ряду занимает «промышленный шпионаж».

Сегодня стало почти массовым явлением беззастенчивое заимствование интеллектуальной и промышленной собственности: сотрудники предприятий, являясь одновременно членами кооперативов, малых предприятий или совместных предприятий, используют методики, программы и технологии, разработанные на отечественных предприятиях и являющиеся их интеллектуальным капиталом. Западные партнеры стремятся незаконным путем . получить закрытую информацию, представляющую для них экономический интерес. Поэтому обеспечение экономической безопасности предприятия, фирмы и любой другой формы хозяйствования в условиях рыночной экономики требует защиты коммерческой тайны.

В США, ФРГ, КНР, Японии и других странах защита коммерческой тайны обеспечивается системой промышленной секретности, которая базируется на соответствующей правовой базе. При этом основную роль в обеспечении ее сохранности играют сами фирмы, а не государственные органы.

Промышленный шпионаж - незаконный сбор сведений, составляющих коммерческую тайну, незаконное использование секретной информации лицом или предприятием, не уполномоченным на то ее владельцем. Объектом промышленного шпионажа могут выступать любые материальные или нематериальные объекты, содержащие коммерческую тайну предприятия: документы, чертежи, образцы продукции, неоформленные патенты, технические проекты, информация о ценах, контрактах, поставщиках, маркетинговых исследованиях и иных сведениях, представляющих предпринимательский интерес.

Коммерческой тайной является информация, которая:

- имеет самостоятельную экономическую стоимость благодаря тому, что не является общеизвестной или доступной людям, которые могут ее использовать в коммерческих целях;

- является объектом разумных усилий по защите. Разумеется, если что-то 'названо коммерческой тайной, , то это действительно должно ею быть, что бывает непросто доказать юридически. Поэтому закон рекомендует:

- указать ценность информации (какие средства затрачены на получение информации и во что обойдется Вам ее несанкционированное обнародование);

- назвать, какие меры защиты данного секрета были предприняты.

Коммерческой тайной, в отличие от производственной, являются сведения, которые касаются торговых отношений фирм: организация и размеры оборота, состояние рынков сбыта, сведения о поставщиках и потребителях, сведения о банковских операциях.

Коммерческие службы безопасности являются хозрасчетными организациями и выполняют определенный вид работ и услуг согласно контрактам, заключаемым с госучреждениями, частными предприятиями. Решение о том, какие секреты необходимо защищать на каждом предприятии, в каждой организации принимается на основе договоренности и строится на экономическом расчете.

Понятие «коммерческая тайна» совсем недавно появилось в нашем законодательстве. Если быть точным, то это признано 12 июня 1990 года, когда был принят Закон «О предприятиях и предпринимательской деятельности».

Согласно ст. 139 Гражданского кодекса Российской Федерации, принятого Государственной Думой 21 октября 1994 года, «информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании и обладатель информации принимает меры к охране ее конфиденциальности».

Разглашение коммерческой тайны может ухудшить экономическое положение предприятия или фирмы. Чтобы этого не произошло, следует перевес-

ти такую информацию в разряд охраняемой. У нас это делается приказом руководителя фирмы, в котором перечисляются сведения, относящиеся к коммерческой тайне. Однако он не вправе отнести к ней сведения, подпадающие под категорию государственной тайны, так как они имеют свой, специальный режим охраны. Кроме того, руководитель фирмы не может отнести к коммерческой тайне сведения о видах деятельности фирмы, поскольку это может привести к сокрытию сведений о загрязнении окружающей среды и другой негативной деятельности, способной нанести ущерб обществу.

Методика отнесения тех или иных сведений к коммерческой тайне в нашей стране еще не разработана, поэтому, опираясь на опыт зарубежных стран, ограничимся лишь некоторыми рекомендациями.

1. При засекречивании информации надо исходить из принципа экономической выгоды и безопасности фирмы .

Причем, объявляя ту или иную информацию коммерческой тайной, важно соблюсти «золотую середину». Чрезмерное засекречивание деятельности фирмы может обернуться потерей прибылей, так как условия рынка требуют широкой рекламы производимой продукции и услуг. Те же результаты может вызвать пренебрежительное отношение к коммерческой тайне, так как рынок - это всегда конкуренция. Американские предприниматели считают, что утрата 20% информации приводит к разорению фирмы в течение месяца в шестидесяти случаях из ста.

2. Информация типа «ноу-хау», безусловно, должна быть отнесена к разряду коммерческой тайны. Ее надо охранять и от собственного персонала, ибо всегда существует опасность, что тот или иной сотрудник уволится и устроится на работу в конкурирующую фирму. Сведения же, которыми он владеет, не могут быть у него изъяты.

За рубежом существует практика подписания с сотрудником соглашения, по которому ему после увольнения запрещается работать в конкурирующей фирме. Правда, такого рода соглашения действуют лишь в течение определенного срока после расторжения договора о найме. Кроме того, во время действия подобного ограничения этому лицу должно выплачиваться вознаграждение. В нашей практике такие соглашения пока неизвестны.

3. Информация о рационализаторском предложении, изобретении, находящегося на стадии разработки, несомненно, относится к коммерческой тайне.

Рационализаторское предложение даже после его оформления и выдачи авторского свидетельства может оставаться коммерческой тайной, поскольку представляет собой техническое решение задачи, новое для данной фирмы.

Изобретение после выдачи на него патента имеет специальную правовую охрану и поэтому не нуждается в защите при помощи коммерческой тайны. Другое дело, если по соглашению с автором изобретения фирма примет решение не подавать заявку в Госпатент Российской Федерации. Тогда охрана информации полностью возлагается ни фирму. Следует подчеркнуть, что решение не подавать заявку на изобретение на патентоспособное техническое решение

возможно только по договоренности с автором, так как по существующему правилу, если работодатель в течение трех месяцев с момента уведомления его автором о сделанном изобретении не подаст заявку не него, автор вправе сам подать заявку и получить патент.

До недавнего времени 90 % авторских свидетельств получали гриф «Для служебного пользования». Вместо авторского свидетельства теперь выдают патент.

Основным принципом патента является его обязательная открытость, что способствует ускорению научно-технического прогресса. Патент - тот же товар изобретателя, но государство продолжает засекречивать патенты, т. е. нарушает права изобретателей. Государство же должно не отбирать у человека право на его интеллектуальную собственность, а выкупать его, причем по рыночной стоимости.

4. Особое внимание следует уделить охране договоров, заключаемых предприятием. Большая их часть, безусловно, относится к коммерческой тайне. Причем в определенных случаях охране подлежит не только текст договора, но и сам факт его заключения.

Разрабатывая меры по защите коммерческой тайны фирмы, необходимо экономически обосновать целесообразность засекречивания той или иной информации.

В первую очередь выделяется информация, утечка которой может привести вашу фирму к банкротству. Это строго конфиденциальная информация. В мире бизнеса это, как правило, «ноу-хау». К конфиденциальной информации относятся сведения о перспективах развития фирмы, ее клиентах, сроках и сумме кредитования. Огласка этих сведений, конечно же, не приведет к краху, но лишит фирму на какое-то время устойчивой прибыли.

Не подлежит огласке информация, раскрытие которой может привести к неблагоприятным последствиям. К ней относятся: номера домашних телефонов, адреса руководителей и сотрудников фирмы, текущие планы работы, информация о конфликтных ситуациях в коллективе.

Остальные сведения относятся к открытым, то есть доступным всем. Но следует иметь в виду, что неправильно поданная информация может помочь аналитикам из конкурирующей фирмы обнаружить ваши уязвимые места.

Руководитель фирмы должен установить строгий порядок хранения первых экземпляров договоров и работы с ними. Их следует хранить в определенном месте у ответственного лица и выдавать только под расписку с письменного разрешения руководителя фирмы. На лица, ответственные за хранение договоров и работу с ними, возлагается персональная ответственность за утерю договоров или утечку информации из них. Все это необходимо потому, что деятельность коммерческих структур строится в большей степени на договорных началах, и конкурент или партнер по переговорам, обладая информацией в этой сфере, может составить довольно полную картину производственного и финансового положения фирмы. Пропажа (похищение) первых экземпляров ведет к

значительным затруднениям и даже невозможности доказывать те или иные положения при возникновении спора и его разрешения в судебном порядке. При подписании договора рекомендуется, чтобы представители сторон ставили подписи не только в конце договора, но и на, каждом листе во избежание замены одного текста другим.

Следует отметить, что затраты зарубежных фирм на охрану своей коммерческой тайны составляют 10-15 процентов всех расходов на процесс производства. Поэтому в наиболее расчетливые предприниматели пытаются на этом сэкономить, переложив затраты на плечи государства. Каким образом? Путем получения госзаказов оборонного характера. Помимо прочих преимуществ, госзаказы позволяют пользоваться защитой государственных правоохранительных органов и, в первую очередь, контрразведки.

Допуская служащих фирмы к госсекретам, контрразведка с присущей ей тщательностью проверяет благонадежность каждого из них.

Традиционная проверка граждан США, получающих доступ к секретной информации, обычно включает:

- обязательную проверку на детекторе лжи (полиграфе);
- глубокое и всестороннее изучение досье кандидата на работу;
- проверка его биографических данных за последние 10 лет;
- выяснение целей и обстоятельств поездок за рубеж;
- исследование финансового положения.

В ходе проверки служащего полученные сведения сопоставляются с данными Национального банка информации о секретоносителях, где на каждого существует электронное досье. В нем содержатся данные предыдущих проверок его фотография, фонограмма его голоса, сведения об изменениях в его финансовом положении, о его поездках за границу.

В Америке служащие многих фирм и всех специальных учреждений проходят проверку на детекторе не реже одного раза в полгода, причем всегда неожиданно. Это обязательное условие оговорено в контракте. По уже сложившейся традиции первым подвергает себя проверке глава фирмы.

Сейчас полиграфы стали предметом многочисленных споров. После того, как в производстве появились бесконтактные детекторы, определяющие состояние исследуемого на расстоянии по голосу, многие заговорили о правах человека. В 1996 году проверки на полиграфе в той или иной мере применялись в 57 странах мира. Но отношение к нему на Западе неоднозначное. В ФРГ, например, он запрещен законом. Видимо, на то есть свои причины. В России же официальные лица делают вид, что детектора лжи у нас не существует. Он не запрещен и не разрешен никакими документам, хотя определенные подвижки к его официальному применению уже имеются.

Закон Российской Федерации «О государственной тайне» предусматривает (ст. 22, ч. 3) «проведение ... полномочными органами проверочных мероприятий» в отношении лиц, получающих допуск к государственной тайне. Определяя основания для отказа гражданам в работе, закон указывает (ст. 22, ч. 1),

что таковыми являются:

- выявление в результате проверочных мероприятий действий оформляемого лица, создающих угрозу безопасности Российской Федерации;

- уклонение его от проверочных мероприятий и (или) сообщение им заведомо ложных анкетных данных.

Таким образом, зафиксирована правовая база для возможного использования в будущем - проверки на полиграфе как дополнительного средства повышения эффективности подбора, перепроверки и расстановки кадров. Закон «О государственной тайне» и введенное Постановлением Правительства Российской Федерации от 5 апреля 1995 года № 333 «Положение о лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны» наметил возможные подходы к развитию данного направления. В опубликованной 24 июня 1996 года «Федеральной целевой программе по усилению борьбы с преступностью на 1996-1997годы» предусматривается «оснастить оперативно-технические и оперативные подразделения республиканских, краевых, областных органов внутренних дел специальными техническими средствами (полиграфами, стресс-детекторами по голосу, тензометрическими платформами) для оценки психофизического состояния человека».

С формированием в России рыночных отношений руководители частных фирм явнее других работодателей осознали значение квалифицированного персонала для развития и процветания своих компаний. Важную роль в оценке пригодности кандидата на вакантную должность стал играть уже не только уровень профессиональной подготовки, но и моральные качества работника.

На какие вопросы работодатель обычно желает получить ответ:

- не имеет ли кандидат на вакантную должность вредных наклонностей (алкоголизм, наркомания);

- не скрывает ли сведения о совершенных в прошлом уголовно наказуемых деяниях;

- верно ли сообщил данные о прежних местах работы;

- лоялен ли по отношению к руководству фирмы;

- не имеет ли каких-либо связей с конкурирующими фирмами;

- не вынашивает ли криминальные замыслы.

Эффективность использования полиграфа для получения ответов на эти и другие подобные вопросы подтверждается как на Западе, так и уже имеющимся опытом в отечественном бизнесе.

Помимо проверки на благонадежность сотрудников коммерческой фирмы, получающих доступ к государственным секретам, контрразведывательные органы формируют систему безопасности фирмы, включая программу защиты, вводят ее в штат своих сотрудников.

Наша экономика находится лишь на этапе становления рыночных отношений, поэтому для коммерческих структур, не связанных с выполнением оборонных заказов, состояние защиты от промышленного шпионажа выглядит удручающим. Ухудшение криминогенной обстановки в стране, усиление межрегиональных связей организованных преступных групп, рост их финансовой мощи и технической оснащенности дает основание полагать, что тенденция к осложнению оперативной обстановки вокруг коммерческих предприятий в ближайшем будущем сохранится. Поэтому необходимо определять и прогнозировать возможные угрозы как основы для обоснования, выбора и реализации адекватных защитных мер. Предлагаемая характеристика угроз безопасности фирмы приведена на рис.2

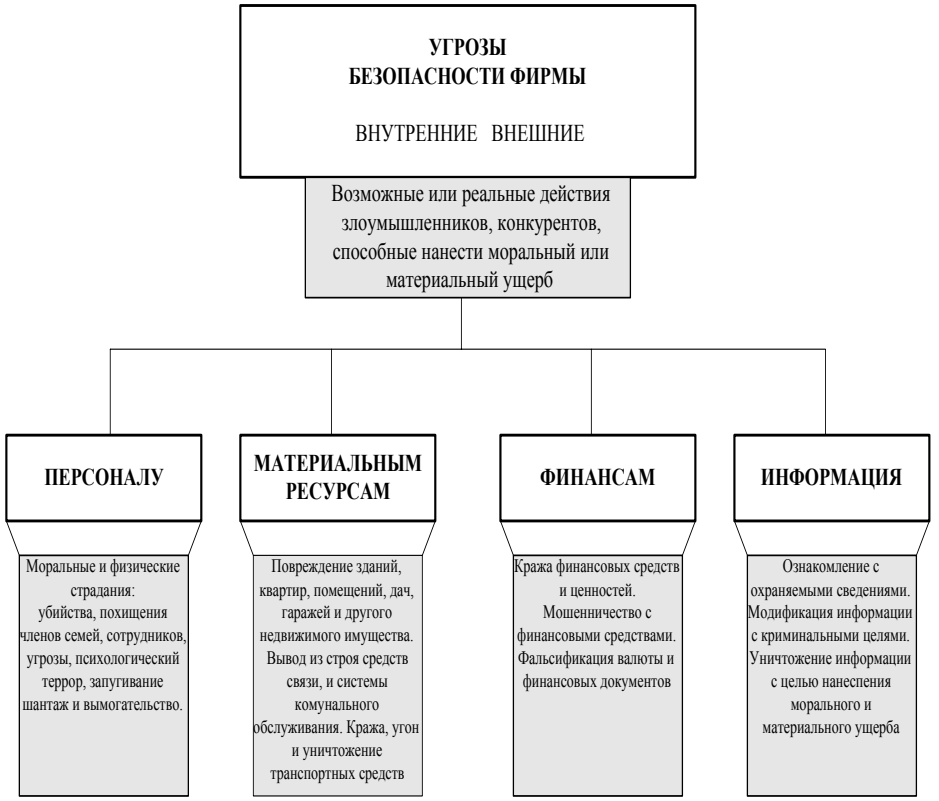

Рис. 2

Что можно рекомендовать руководителю, начинающему создавать систему безопасности на своей фирме? Прежде всего, знать, что это обойдется недешево. Поручить создание системы безопасности профессионалам, только им, и никому более. Сразу же следует подумать о безопасности наиболее важных секретов, утечка которых способна нанести ущерб, значительно превышающий затраты на их защиту. При этом надо установить:

- какая информация нуждается в защите;
- кого она может заинтересовать;
- каков «срок жизни» этих секретов;
- во что обойдется их защита. Затем следует подготовить план по охране коммерческой тайны. Основываясь на зарубежном опыте, он должен состоять из двух разделов:
- предотвращение похищения секретной информации;
- предотвращение утечки секретной информации.

Для этого требуется:

- определить, какая коммерческая информация является секретом фирмы;
- установить места ее накопления;
- выявить потенциальные каналы утечки информации;
- получить консультацию по перекрытию этих каналов у специалистов;
- проанализировать соотношение затрат по использованию различных систем, обеспечивающих защиту секретной информации, и выбрать наиболее приемлемую;
- назначить людей, ответственных за каждый участок этой системы;
- составить график проверки состояния дел на участках.

Система обеспечения безопасности фирмы включает в себя следующие организационные мероприятия:

- контроль помещений и оборудования (обеспечение безопасности производственных и конторских помещений, охрана фото- и иного копировального оборудования, контроль за посетителями);
- работа с персоналом (беседы при приеме на работу, ознакомление вновь принятых с правилами защиты информации, обучение сохранению коммерческой тайны, стимулирование соблюдения коммерческой тайны, работа с сотрудниками, подозреваемыми в хищении секретной информации, беседы с увольняющимися);
- организация работы с конфиденциальными документами (установление порядка делопроизводства, контроль за прохождением секретных документов, контроль за публикациями, рассекречивание и уничтожение конфиденциальных документов, охрана секретов других фирм);
- работа с конфиденциальной информацией, накопленной в компьютерах фирмы (создание системы защиты электронной информации от несанкционированного доступа, обеспечение контроля за пользованием ЭВМ);
- защита коммерческих тайн фирмы в процессе заключения контрактов (здесь важно четко определить круг лиц, имеющих отношение к этой работе).

Вышеизложенный план является примерным. Однако, во всех случаях защиты коммерческой тайны необходимо обратить особое внимание на документы, поскольку в нашей стране основные объемы коммерческой информации хранят в документах.

Руководитель должен упорядочить процессы фиксации секретной информации в деловых бумагах и организовать их движение таким образом, чтобы похищение конфиденциальных документов было бы затруднено настолько, чтобы оно становилось экономически невыгодным для похитителя. При работе с документами, содержащими коммерческую тайну, следует соблюдать определенные правила, которые сводятся к нижеследующим:

- строгий контроль (лично или через службу безопасности) за допуском персонала к секретным документам;
- назначение ответственных лиц за контролем секретного делопроизводства и наделение их соответствующими полномочиями;
- разработка инструкции (памятка) по работе с секретными документами, ознакомление с ней соответствующих сотрудников фирмы;
- контроль за принятием служащими письменных обязательств о сохранении коммерческой тайны фирмы;
- введение системы материального и морального поощрения сотрудников, имеющих доступ к секретной информации;
- внедрение в повседневную практику механизмов и технологий защиты коммерческой тайны фирмы;
- личный контроль со стороны руководителя фирмы за службами внутренней безопасности и секретного делопроизводства.

Существуют различные способы ведения секретного делопроизводства, которые направлены на предотвращение утечки содержащихся в документах коммерческих секретов. Как уже было указано выше, документы, содержащие коммерческую тайну, подразделяются по степени секретности имеющейся в них информации и снабжаются соответствующим грифом секретности.

Грамотно поставленная работа с документами поможет защитить их от постороннего глаза. Не следует держать на столе сразу несколько документов, до к тому же различных по степени значимости.

При работе с документами не отлучайтесь из комнаты, а если приходится выходить, то не забудьте закрыть дверь.

Посторонних к документам допускать не следует. Документы, которые правомерно могут потребовать сотрудники налоговой инспекции или правоохранительных служб, следует держать отдельно от остальных конфиденциальных бумаг. По окончании работы наиболее важные документы убираются в сейф, менее важные - в специальные контейнеры. Те и другие следует опечатать и сдать на хранение сотрудникам службы безопасности фирмы.

При пересылке документов следует иметь в виду, что использование телемониторов-игл позволяет через непроклееные уголки конвертов прочитать содержимое делового письма, не вскрывая его. Поэтому конверты с документа-

ми целесообразно дополнительно проклеить скотчем.

Доверяя свои бумаги почте, отправляйте их заказными письмами и письмами с уведомлением о вручении их адресату.

Перемещение документов внутри фирмы также следует держать под контролем.

Организация защиты документов - обязанность руководителей фирмы и ее службы безопасности. Следует быть уверенным, что с момента появления и до уничтожения документ к посторонним не попадал. Если документ утерян (украден), специалисты по службе безопасности должны провести расследование.

Подготовку документов, содержащих важные сведения, следует доверять проверенным людям. Количество экземпляров должно быть строго ограниченным. Для разделения документов по степени важности можно использовать яркие цветные наклейки. При необходимости следует определять степень конфиденциальности документа, а также срок действия ограничительных грифов. При этом необходимо помнить: чем больше секретной информации в нем отражено, тем больше потребуется затрат для его защиты.

Копирование документов - один из способов получения сведений, составляющих тайну фирмы. Множительная техника должна находиться под надежным контролем. Количество копий должно строго учитываться, а их уничтожение - контролироваться. Придерживайтесь правила; наиболее ценные документы руководители фирм копируют сами.

Если документы размножаются на принтерах ЭВМ, то следует позаботиться о защите информации на магнитных носителях. Если это пишущая машинка нового поколения, то следует принять меры по хранению перфоленты, позволяющей повторно печатать один и тот же текст в автоматическом режиме. По стуку клавишей пишущей машинки специалист с помощью электроники получит текст, аналогичный оригиналу, находясь вне помещения вашего офиса.

Для работы с секретными документами должны отводиться специальные помещения с хорошей звукоизоляцией. В эти помещения не должны допускаться не только посторонние лица, но и сотрудники, не имеющие разрешения (допуска) на работу с секретами фирмы. Эти помещения должны иметь капитальные стены, надежные перекрытия, прочные двери с замками и запорами, защиту на окнах от проникновения посторонних лиц. Эти помещения должны надежно охраняться, в том числе системой охранной сигнализации, электронно-механическими приспособлениями, системами кабельного телевидения.

Черновики секретных документов должны готовиться в тетрадях с пронумерованными листами. После подготовки документов «набело» черновики должны уничтожаться уполномоченными на то сотрудниками. Число копий секретных документов должно строго учитываться, а копировальные машины снабжаться счетчиком копий и ключом, запускающим машины в действие.

Копировальная бумага и красящая лента пишущих машин - предмет особых забот, так как с них можно снять секретную информацию. Поэтому исполь-

зованная копировальная бумага и лента уничтожаются под контролем ответственных лиц.

Вероятность утечки секретной информации из документов особенно велика в процессе их пересылки. Если нет возможности пользоваться услугами военизированной фельдсвязи, то доставку секретных документов и ценностей следует организовать своими силами с привлечением сотрудников собственной службы безопасности или же обратиться в специализированные фирмы, которые такие услуги оказывают за плату.

Служащие фирмы, отвечающие за сохранность, использование и своевременное уничтожение секретных документов, должны быть защищены от соблазна торговли секретами фирмы простым, но весьма надежным способом - хорошей зарплатой.

В процессе хранения и пересылки секретных документов могут быть применены средства защиты и сигнализации при несанкционированном доступе к ним. Одна из новинок - светочувствительное покрытие, наносимой на документы, которое может проявиться под воздействием света, указывая тем самым на факт ознакомления с документами или их фотографированием посторонними лицами.

Используют в этих целях и электронику. Электронное устройство величиной со спичечный коробок реагирует на свет. Стоит его включить и поместить в сейфе, под бумагами на рабочем столе - и в вашем распоряжении надежный сторож.

Специалистам по вопросам защиты коммерческой информации известны и иные технологии и системы охраны конфиденциальных документов от несанкционированного доступа или возможной утечки из них охраняемых сведений.

С коммерческой тайной связано такое понятие, как интеллектуальная собственность, которое в широком смысле слова может быть определено как коммерчески ценные идеи. Не обязательно, чтобы это было что-то новое или запатентованное. Главное, чтобы информация не относилась к числу общеизвестной.

Впервые понятие «интеллектуальная собственность» прозвучало у нас в 1990 году в тексте Закона о собственности в РСФСР. А вообще оно существует с 1967 года, когда на Стокгольмской конференции была создана Всемирная организация интеллектуальной собственности, к которой недавно присоединилось и наше государство. До этого собственностью считалось только то, что можно взять в руки, потрогать или на что можно посмотреть. Наше руководство не задумывалось над тем, какой поистене бесценной интеллектуальной собственностью располагает страна, и что беречь ее надо не меньше, чем золотой запас. Этому свидетельствует целый ряд горьких уроков. Притчей во языцех стал метод непрерывной разливки стали, изобретенный у нас и успешно используемый во всем мире для возвращения которого на Родину пришлось заплатить немалые деньги. В стране создано большое число лекарственных препаратов, секре-

ты которых уплыли за рубеж, и сейчас мы вынуждены покупать патенты на их производство. Японский бизнесмен тепло поблагодарил журнал «Юный техник» за его приложение «Сделай сам». Используя чертежи, помещенные в этом издании, он заработал миллионы долларов. И подобным примерам нет числа.

Новые идеи - специфический товар, имеющий коммерческую стоимость. В отличие от материальных вещей, которые постоянно обладают стоимостью, сколько бы раз их ни производили, стоимость идей одноразовая (никто не будет платить за уже известные сведения).

Интеллектуальная собственность имеет не только реальную стоимость, в которую входят затраты на получение информации и ее защиту, но и потенциальную стоимость (возможная прибыль при ее реализации). В качестве несколько неожиданного примера информации, имеющей потенциальную стоимость, можно привести «негативную информацию» (о том, что не надо делать), которая позволяет не расходовать средства на тупиковые разработки.

Сегодня уровень конкурентоспособности в немалой степени зависит от умения защитить свою деловую и техническую информацию от хищений, несанкционированного использования, изменения или уничтожения.

3. ДОКУМЕНТООБОРОТ И ОБЕСПЕЧЕНИЕ ЗАЩИТЫ СЕКРЕТНОЙ ИНФОРМАЦИИ

Промышленный шпионаж приобрел гигантский размах.

По оценке экспертов, ежегодный урон американского бизнеса от кражи производственных и торговых секретов превышает четыре миллиарда долларов.

Кроме прямого похищения, происходит и утечка информации, при этом наиболее вероятными ее источниками являются:

- персонал, имеющий доступ к информации;
- документы, содержащие эту информацию;
- технические средства и системы обработки информации, в том числе линии связи, по которым она передается.

Концептуальная модель защиты информации при защищенном документообороте приведена на рис. 3

Итак, персонал - один из главных каналов утечки информации. Зная это, следует более тщательно изучать биографии особо важных сотрудников. Следует обратить пристальное внимание как на вновь пришедших на работу, так и на тех, кто подлежит увольнению. Эти люди находятся в ситуации, наиболее благоприятных для утечки информации.

Возможными источниками утечки интеллектуальной собственности могут стать конгрессы, конференции, симпозиумы, торговые выставки, демонстрации созданной техники, ярмарки, реклама и т. п. Профессионалов промышленного шпионажа привлекают и различные съезды специалистов, потому что они знают: самые лучшие источники коммерческой и научно-технической информации - болтуны.

Утечка информации охватывает широкий круг различных действий. Это

и утрата информации из компьютера, и пропажа документов. Утратой считается и тайное копирование информации конфиденциального характера с дискеты на дискету, снятая "лично для себя" копия документа, содержащего коммерческую тайну.

Концептуальная модель
защиты информации
при защищенном документообороте

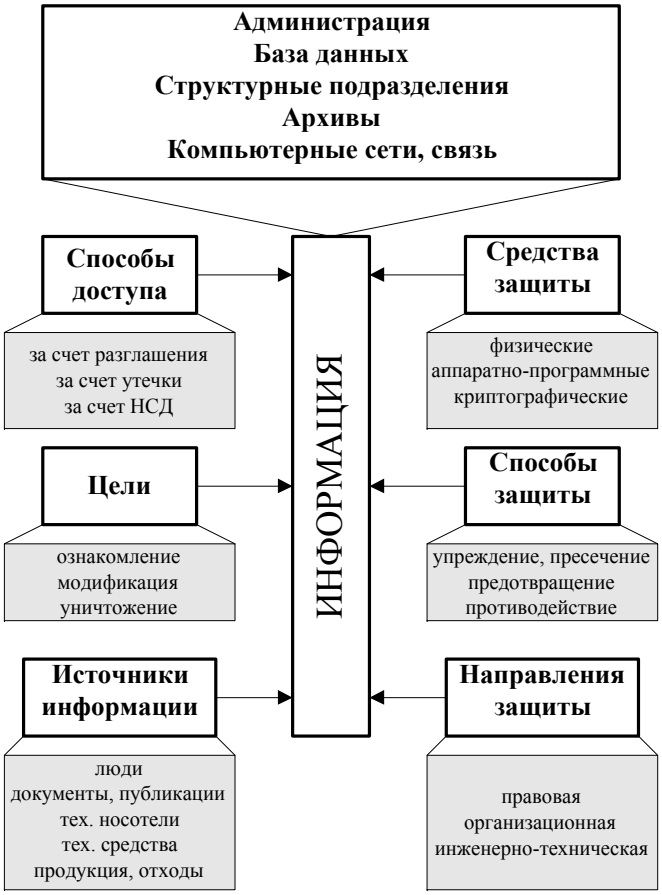

Рис. 3

Существуют три общепринятых метода защиты интеллектуальной собственности: патент, авторское право и коммерческая тайна.

Патентом оформляется право изобретателя «законно монополизировать» использование изобретения в течение установленного периода времени. Основами гражданского законодательства срок действия патента определен в 20 лет. Патент является способом защиты промышленной, а не коммерческой информации.

Авторское право, напротив, защищает только форму, в которой выражена конкретная идея, а не саму идею. Это отличает авторское право и от патента, и от коммерческой тайны, которые относятся к сущности, содержанию идеи. Оригинальные мысли, содержащиеся в книгах и научных статьях, после их прочтения уже принадлежат каждому. Ими можно свободно пользоваться. Однако при использовании этих идей в новых публикациях необходимо делать ссылки на конкретного автора, иначе будут нарушены авторские права. Это относится в большей степени к литературному творчеству, музыке, программному обеспечению.

Коммерческая тайна как форма интеллектуальной собственности в нашей стране не охвачена правовым регулированием, поэтому для защиты коммерческой информации применение законодательных мер значительно осложнено, и здесь большое значение приобретают другие меры защиты.

Немаловажную роль в защите информации играют **морально-этические нормы,** которые не являются обязательными, однако их несоблюдение ведет к потере авторитета (престижа) человека, группы лиц либо всей организации.

При охране информации от прямого хищения или уничтожения нередко прибегают к мерам **физической защиты.** Это - замки на дверях, решетки на окнах, различные механические, электромеханические и электронные устройства охраны здания, лаборатории, других помещений фирмы.

Физические меры защиты, как правило, применяются в совокупности с **административными мероприятиями.** К ним относятся: организация соответствующего режима секретности, пропускного и внутреннего режима, создание службы безопасности, обучение и инструктаж персонала.

Технические системы охраны включают в себя электромеханические, акустические, емкостные, радиотехнические, магнитометрические средства.

Криптографические меры защиты позволяют шифровать информацию таким образом, чтобы ее содержание, могло стать доступным только при предъявлении специфической информации (ключа). Специалисты считают криптографическое закрытие информации наиболее эффективным и надежным средством.

В качестве потенциальных угроз безопасности информации могут выступать стихийные бедствия, неблагоприятная внешняя среда, катастрофы, политическая нестабильность, ошибки и неисправности программы, компьютерная преступность. Концептуальная модель угроз безопасности информации при

защищенном документообороте приведена на рис. 4

Концептуальная модель угроз безопасности информации при защищенном документообороте

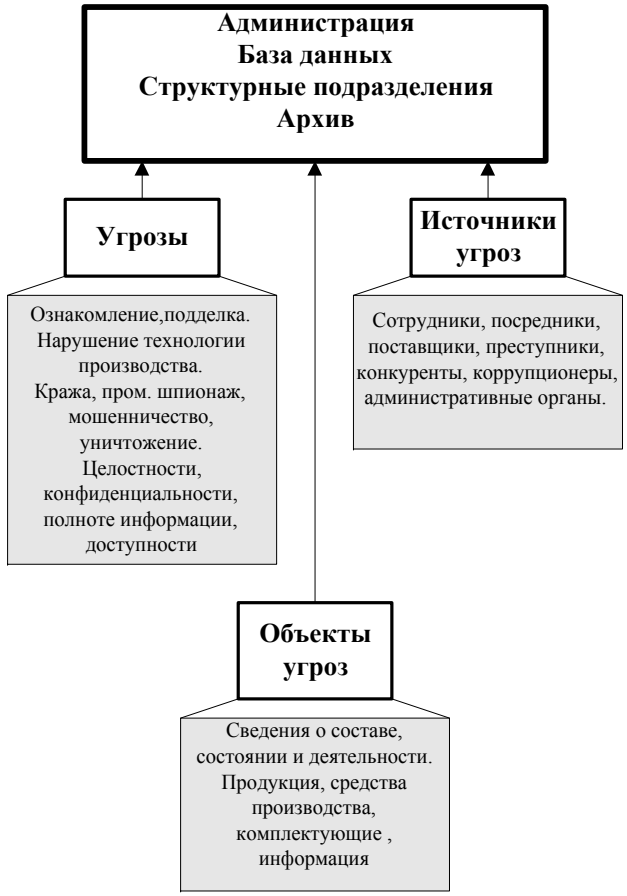

Рис. 4

Исходя из характера угрозы, применяются различные меры противодействия.

Для защиты коммерческих секретов следует соблюдать следующие правила:

- обеспечение безопасности всегда и везде - дело профессионалов, потому что для этого требуются специальные знания;
- предпринимаемые превентивные меры должны предусматривать специ-

альную программу по дезинформации промышленных, шпионов;

- система превентивных мер должна включать в себя такой важнейший элемент, как организация движения охраняемой информации, исключив при этом возможность её утечки;

- система превентивных мер должна быть основана на материальной заинтересованности сотрудников, а для этого надо адекватно оплачивать их труд. В нашей стране такую систему превентивных мер по защите коммерческой тайны могут позволить себе пока что немногие частные фирмы.

Объективные потребности фирмы, банка, страховой компании в обеспечении сохранности коммерческой тайны определяются рядом факторов, а именно:

- обострением конкурентной борьбы на рынке товаров и услуг;

- важностью сохранения секретной информации в течение определенного времени;

- возможностью проверить каждый из вероятных каналов утечки информации, и в первую очередь по конкретным служащим.

Последние два фактора должны быть тщательно просчитаны по затратам: стоит ли овчинка выделки?

На начальной стадии создания фирмы, когда ее штат ограничен несколькими сотрудниками, а финансовые возможности не позволяют осуществить весь комплекс мер по защите информации, складывается ситуация, при которой любые действия конкурентов несут реальную угрозу гибели фирмы. На этой стадии необходимо осуществить хотя бы минимально возможный комплекс мер:

- предусмотреть, чтобы служащие в заявлениях о приеме на работу, в трудовых соглашениях и контрактах принимали на себя четко выраженные письменные обязательства не разглашать тайны фирмы и иные сведения, ею охраняемые;

- определиться с потоками информации и все документы, содержащие коммерческую тайну, снабдить соответствующим грифом, отражающим степень их секретности. Сюда относятся, прежде всего, документы с планами предстоящей деятельности фирмы, технологическая документация, списки поставщиков и покупателей;

- предусмотреть вопросы защиты коммерческой тайны в типовых соглашениях с заказчиками, покупателями изделий и услуг фирмы, продавцами, торговыми агентами и др.

В промышленно развитых странах основой защиты коммерческой тайны являются законодательные акты и контракты найма-увольнения, заключаемые служащими с фирмой. Даже при наличии соответствующих законов многие фирмы идут на то, чтобы подписывать контракты со своими служащими о неразглашении доверенных им, секретов либо с момента установления трудовых отношений, либо когда сотрудник получает доступ к коммерческим секретам.

В условиях, когда правового регулирования охраны коммерческой тайны

еще не существует, хотя кое-какие проекты уже разработаны, следует обусловить принятие на себя служащим фирмы, работающим по контракту, обязательства о неразглашении коммерческих секретов, при этом данный документ должен прямо предусматривать право работодателя расторгнуть трудовое соглашение (контракт) с сотрудником, нарушившим названное обязательство, а также принимать иные меры, предусмотренные законом.

В странах, где нормы права довольно детально регламентируют охрану коммерческой тайны, тем не менее общеприняты типовые формы соглашений (контрактов) о ее неразглашении. Рассмотрим форму документа, рекомендованную по защите деловой информации в Соединенных Штатах Америки.

Соглашение о неразглашении коммерческой тайны

Приступая к выполнению своих обязанностей в качестве служащего Компании, я понимаю, что получу доступ к информации, касающейся ее бизнеса. Я также понимаю, что во время работы будут заниматься анализом, составлением схем, таблиц, чертежей, докладов и других конфиденциальных документов, относящихся к делам Компании.

В связи с этим даю обязательство, что ни во время моей работы, ни после увольнения не буду обсуждать с кем-либо или раскрывать (за исключением случаев выполнения своих обязанностей в качестве служащего Компании) какую-либо информацию или коммерческие секреты, полученные или разработанные мною. Я также согласен с тем, что все аналитические разработки, схемы, чертежи, доклады и другие документы, подготовленные лично мною либо в сотрудничестве с другими служащими, являются собственностью Компании. Обязуюсь, что не буду сам и не позволю никому другому снимать копии или делать аннотации с вышеупомянутых документов.

Я подтверждаю, что не не имею перед кем-либо никаких обязательств, которые входят в противоречие с настоящим Соглашением или ограничивают мою деятельность в Компании.

Дата *Подпись Служащего*

Дата *Подпись Свидетеля*

Конечно, служащий фирмы, подписывая подобного рода документ, должен четко представлять, что конкретно из деловой информации и технологических разработок является тайной фирмы. Как раз по этой причине и считается обязательным требование о том, чтобы вся секретная информация была обособлена от остальных сведений, а документы, ее содержащие, носили соответствующий гриф.

Приведенный выше текст соглашения о сохранности коммерческой тайны, по мнению американских юристов, оставляет многие вопросы без ответа. На практике для охраны коммерческой тайны фирмы ее служащими как во

время работы в ней, так и после увольнения, используются более детально проработанные соглашения. Важно, чтобы условия сохранения коммерческой тайны бывшим сотрудником фирмы были реальными по времени, оставляя ему возможность подыскать достойно оплачиваемую работу.

Использование контрактов о сохранении коммерческой тайны позволяет обеспечить формальную юридическую защиту коммерческой информации, к которой имеет или имел доступ персонал фирмы.

Однако коммерческие тайны полностью или частично могут стать известны деловым партнерам вашей фирмы в процессе обмена с ними необходимой для совместной работы информацией. Следовательно, они должны принять на себя обязательства по защите ваших коммерческих тайн, равно как и вы должны поступить таким же образом в отношении их. Это традиционная для делового мира практика, но и она должна подкрепляться письменными обязательствами.

Соглашение о сохранности коммерческой информации

Здесь и далее «Доверяющий» или Ваше имя, здесь и далее «Доверенный» желают рассмотреть возможность для чего необходимо, чтобы Доверенный имел доступ к информации о_____

_____

Эта информация составляет коммерческую тайну Доверяющего и раскрывается только в заранее оговоренных целях. Доверенный обязуется сохранять в секрете эту информацию и не использовать ее в других целях. Доверенный обязуется ознакомить под роспись с этим Соглашением всех своих сотрудников, которые получат доступ к данной информации. По окончании переговоров (или сотрудничества) Доверенный сразу же вернет все материалы, содержащие данную информацию, Доверяющему.

Это соглашение не относится к информации, законным владельцем которой является Доверенный, или информации, полученной им у третьих лиц.

Дата *Подписи*

Готовя документы на приобретение каких-либо товаров или услуг, размещая заказы на них, следует в соответствующих соглашениях или договорах обязательно указать, что продавец (поставщик) обязуется содержать в секрете всю предоставленную ему в связи с данным заказом вашу информацию. По исполнении заказа все документы фирмы, содержащие секретную информацию, он обязуется возвратить во взаимообусловленные сроки.

Рекомендуется на документах с конфиденциальной информацией, адресуемой поставщикам фирмы, ставить штамп, который свидетельствовал бы о том, что изложенные в документе сведения являются частной собственностью фирмы и требуют соответствующей защиты и своевременного возвращения владельцу.

Соглашение о сохранении коммерческой информации следует подписать

и с теми партнерами, которые предоставляют фирме разного рода сервисные услуги (ремонт оборудования, уборка помещений).

Если фирма прибегает к услугам торговых посредников или нанимает торговый персонал, то и в этом случае единственной возможностью сохранения коммерческих секретов будет подписание с ними соответствующего контракта.

Нет иных путей для сохранения коммерческих секретов производимой (реализуемой) фирмой продукции (товаров) в общении с контрагентом, кроме как заключение соответствующего соглашения о сохранении коммерческой тайны. Такие сведения могут быть нужны ему, например, для того, чтобы оценить ваши возможности по наращиванию производства данного вида продукции (товара), и краткое соглашение о сохранении тайны заставит его беречь полученную информации.

Таким же образом охраняются коммерческие тайны третьей стороны, в частности вашего поставщика.

Деловые партнеры могут высказать пожелание о предоставлении им всей коммерческой информации для оценки реального состояния ваших дел. На предварительной стадии обсуждения сделки следует воздерживаться от детального обсуждения вашей охраняемой информации. Это возможно лишь после подписания соглашения о сохранении тайны.

В целом же защита коммерческих тайн фирмы в общении с дружественными, лояльными лицами, или же занимающими по отношению к вашему бизнесу нейтральную позицию, осуществляется на основе заключения соответствующих соглашений, прямо предписанных в нормах права, либо так или иначе основанных на них.

Даже тщательно охраняемые тайны фирмы могут стать известны вашим конкурентам из обычных публикаций для широкой публики, если пустить это дело на самотек. Поэтому один из сотрудников должен предварительно просматривать готовящиеся к печати брошюры, рекламные объявления, пресс-релизы и иные материалы, предназначенные для симпозиумов, конгрессов, выставок, а также выступления, научные и иные публикации сотрудников вашей фирмы. Он должен руководствоваться простым, но достаточно эффективным правилом, суть которого состоит в том, чтобы в максимально возможной степени раздробить, разобщить по времени и по авторам ту строго охраняемую коммерческую информацию, без которой невозможно опубликование упомянутых выше работ. Все это существенно препятствует сбору секретной информации о фирме конкурентами или недоброжелателями. Конечно, этот барьер преодолим, но лишь посредством очень больших затрат.

Трудно найти золотую середину между стремлением сохранить коммерческую тайну и желанием использовать в рекламных целях наиболее впечатляющие данные из строго охраняемой информации, особенно те из них, которые, несомненно, помогли бы расширить сбыт производимых товаров и услуг.

Рассмотрим теперь вопрос о том, где и как предприниматель может получить необходимые ему сведения о клиентах и конкурентах, дающие ему воз-

можность нормально работать в условиях рыночной экономики. Известно, что обладание такими сведениями по сути своей есть один из элементов системы превентивных мер по борьбе с промышленным шпионажем.

В капиталистических странах сведения о клиентах принято считать не коммерческой тайной фирмы, а, скорее, ее капиталом. Поэтому список клиентов фирмы и иные сведения о них составляются, в первую очередь, усилиями руководителя и эта информация не доверяется даже его ближайшему окружению.

На каждого клиента фирмы накапливается информация, где отражаются его привычки, характерные черты поведения, его интересы в личной жизни, о предоставляемых ему фирмой привилегиях. Отражаются сведения о его требованиях к качеству и количеству товаров и услуг, какие режимы доставки товаров применялись, какова периодичность поставок, сведения об особенностях платы и иных специфических чертах контрактов с данным клиентом. Здесь отражаются те сведения, которые определяют прибыльность всей операции с ним, какие предполагаются объемы сделок, частота поставок.

Сведения о деятельности фирмы и ее руководителях собирают в различных экономических газетах и журналах, справочниках, выпытывают у биржевиков, покупают у частных детективов.

Осведомленность о наиболее выгодных клиентах конкурента дает шанс победить в состязании с ним, если вам удастся «переманить» его клиентуру. Здесь на первый план выступает персонифицированная информация о клиентах, сведения о симпатиях и антипатиях, об их привязанностях, дружеских связях в среде предпринимателей и их конкурентах, которые влияют на принятие ими решений о поддержке деловых отношений с вашей фирмой или об их прекращении. Сбор информации о клиентах и конкурентах должен быть упорядочен самым тщательным образом, и эта информация должна находиться только у руководства фирмы.

Сотрудники фирмы, продвигающие на рынок ее продукцию, должны представить письменные отчеты о конкретных клиентах по каждому факту продаж. В этих отчетах должны быть отражены перспективы будущих сделок.

Если вашей фирме по силам затраты на содержащие аналитического отдела, изучающего конъюнктуру рынка, клиентов, конкурентов, то и в этом случае следует распределять такого рода конфиденциальную информацию среди сотрудников.

Документация об этом должна быть строго секретной, а персонал, работающий с ней, должно соблюдать правила обращения с секретными документами. Все служащие, работающие непосредственно с клиентами, должны дать письменные обязательства сохранять коммерческие тайны фирмы.

Аналитический отдел или отдел маркетинга, изучая клиентов, должен одновременно собирать и анализировать сведения о конкурентах. Для этого должна быть разработана программа действий каждого сотрудника отдела. Следует четко знать, какие сведения надо получить и где они концентрируются.

Кто и каким образом может добыть эти сведения с наименьшими затратами. Какие трудности могут . возникнуть при этом и как их следует преодолевать. Обязательно следует фиксировать: где, когда и как получена данная информация, кем конкретно и что по ней сделано.

В наших условиях добывание достоверной информации о клиентах и конкурентах - предмет постоянной головной боли. Рынок, его информационные структуры - еще в стадии формирования, притом на самых первых ступенях, По этой причине решение проблемы, вероятнее всего, может осуществляться:

- собственными силами (создание отделов маркетинга, изучения спроса);

- получением за плату нужной информации у тех коммерческих структур, которые ею располагают (банки, страховые компании, биржи, частные детективные агентства);

- обращением за помощью, разумеется, платной, к службам промышленной контрразведки, к частным сыскным агентствам.

Предприниматель осуществляет выбор сам, но в любом случае выбор этот потребуется сделать, потому что система превентивных мер, обеспечивающая безопасность фирмы, без исчерпывающей информации о ее клиентах и конкурентах существовать не может, а сама фирма в таких условиях обречена на проигрыш в конкурентной борьбе.

Добывая жизненно важную коммерческую информацию, не следует забывать, что ваши конкуренты озабочены тем же. Во Франции, например, за промышленными секретами охотятся десятки тысяч промышленных шпионов и на оплату их труда французские бизнесмены ежегодно тратят свыше одного миллиарда долларов.

Следует не забывать о работе с представителями средств массовой информации, тем более что наше законодательство никак не защищает предпринимателей от журналистов.

Исходя из Закона Российской Федерации от «О средствах массовой информации» от 27 декабря 1991 года, не допускается использование средств массовой информации «... для разглашения сведений, составляющих государственную или иную специально охраняемую законом тайну». Но закон о печати не предусматривает ответственности за возможность нанесения публикацией даже существенного имущественного вреда посредством разглашения коммерческих тайн предпринимателей.

Столь существенный недочет Закона «О средствах массовой информации» заставляет любого предпринимателя быть настороже при общении с журналистами. Следует исходить из известного правила: минимум информации - максимум общественного интереса.

Для постоянного общения с представителями средств массовой информации и общественности следует назначить компетентного, толкового сотрудника, умеющего общаться с людьми, располагать их к себе, быстро реагировать на изменяющиеся обстоятельства.

Итак, что же относится к коммерческой тайне и требует защиты от утеч-

ки информации и ее похищения?

1. Деловая информация:

- финансовые сведения;
- данные о цене (стоимости) продукции и услуг, технологии;
- деловые планы и планы производства новой продукции;
- списки клиентов и продавцов, контракты, преференции и планы;
- информация о маркетинге;
- соглашения, предложения, квоты;
- списки персонала, организационные схемы и информация о сотрудниках (их характеристики).

II. Техническая информация:

- научно-исследовательские проекты;
- конструкторские разработки по производству какой-либо продукции и ее технические параметры;
- заявки на патенты;
- дизайн, эффективность и возможности производственных методов, оборудования и систем;
- информационный процесс;
- программное обеспечение ЭВМ;
- химическая формула.

Анализируя зарубежный опыт по созданию механизма защиты коммерческой тайны, можно выделить основные блоки, из которых он состоит:

- нормы права, направленные на защиту интересов ее владельцев;
- нормы, устанавливаемые руководством предприятия, фирмы (приказы, распоряжения, инструкции);
- специальные структурные подразделения, обеспечивающие соблюдение этих норм (подразделение режима, службы безопасности).

Мировой опыт в области защиты производственных секретов показывает, что чисто административные меры не гарантируют результат, поэтому предприниматели, не отказываясь от административных мер, переходят к совмещению их с активным вовлечением в процесс защиты конфиденциальной информации всех сотрудников фирмы.

Главное место в организации надежной защиты секретной информации должно отводиться работе с кадрами. Специалисты считают, что сохранность секретов на 80% зависит от правильного подбора, расстановки и воспитания кадров. И эта работа должна начинаться со дня приема человека на работу.

Вторым по важности мероприятием должно быть ограничение доступа к секретной информации. Работа должна быть организована таким образом, чтобы каждый сотрудник имел доступ только к той информации, которая необходима ему в процессе выполнения прямых служебных обязанностей. Эта мера не сможет сама по себе полностью защитить от возможной ее утечки, но возводит свести возможный ущерб к минимуму.

Третьим направлением в работе с кадрами является проведение воспи-

тательной работы. Специалисты в области противодействия промышленному шпионажу дают следующие рекомендации:

- использовать любую возможность для пропаганды программ обеспечения режима секретности;
- всемерно стимулировать заинтересованность сотрудников в выполнении режима секретности;
- не забывать периодически вознаграждать сотрудников за успехи в защите секретной информации.

Следует иметь в виду, что голые призывы не дают положительных результатов, поэтому значительное место в воспитательной работе необходимо отводить обучению, целями которого являются:

- четкое знание сотрудником объемом охраняемой информации, за безопасность которой он несет личную ответственность;
- понимание исполнителем секретных работ характера и ценности данных, с которыми он работает;
- обучение правилам хранения и защиты секретных данных.

При этом ни одно правило или процедура не должны вводиться без разъяснения их сути, их разумности и необходимости. Каждый руководитель, доводя такие правила до сведения своих подчиненных, обязан подчеркнуть, что они являются неотъемлемой частью их работы.

Вместе с тем не следует ограничиваться только воспитательной работой и обучением. Сотрудник, нарушивший правила работы с секретной информацией, должен знать, что у него будут серьезные неприятности и он будет строго наказан руководством.

Такие подходы к работе с кадрами дают неплохие результаты и могут применяться на предприятиях разного профиля деятельности.

Важным направлением в организации работы по защите конфиденциальной информации является установление порядка обращения с ее носителями, такими как документы, чертежи, дискеты, компьютерные программы и т. п. При этом следует учитывать, что:

- специалисты ставят обязательным условием наличие на носителях конфиденциальной информации отличительных пометок, различающихся в зависимости от уровня секретности, но они должны отличаться от применяемых в сфере защиты государственных секретов;
- в условиях фирмы обеспечить каждому исполнителю работу в специально выделенном помещении бывает практически невозможно, поэтому следует соблюдать «политику чистых столов». Суть ее заключается в том, что в отсутствие работника на его рабочем месте не должно быть никаких документов.

Как показывает практика, значительная утечка коммерческой информации происходит в ходе ведения переговоров. Это объясняется разными причинами: неверно понимаемый престиж, неумение правильно отрекламировать свою продукцию и т. д. Большую роль играет умение ведения переговоров. Со-

трудник должен четко знать, какую информацию он имеет право сообщить партнеру по переговорам, а какую - нет. Необходимо учить проведению рекламы по методу «черного ящика», т. е. можно сообщить параметры изделия, полученный результат, а как он получен - секрет фирмы. Сотрудник должен понимать, что от успешно проведенных переговоров зависит не только процветание фирмы, но и его личное благополучие. Ключевая роль в структуре подразделения, занимающегося защитой коммерческой тайны, должна отводиться аналитической службе. Современное предприятие, функционирующее в условиях рыночной экономики, разумеется, не может позволить себе засекречивать всю информацию. Это слишком дорого и невыгодно: определенная часть сведений должна использоваться в рекламе, к тому же большое количество засекреченных материалов создает помехи в работе.

Специалисты в области стратегического планирования и управления производством относят сбор информации о конкурентных фирмах и компаниях к обычному маркетингу, также как и информацию о потенциальных потребителях, репутации фирмы, государственном регулировании на рынке и т. п.

Существуют три основных направления сбора информации.

1. Информация о рынке:

- цена, условия договоров, спецификация продукта, скидки;
- объем, тенденция и прогноз сбыта конкретного продукта;
- доля на рынке и тенденция ее изменения;
- рыночная политика и планы;
- отношение с потребителями и репутация;
- численность и расстановка торговых агентов;
- каналы, политика и методы сбыта;
- постановка рекламы.

II. Информация о производстве продукции:

- оценка качества и эффективности;
- номенклатура изделий;
- технология и оборудование;
- уровень издержек;
- производственные мощности;
- способ упаковки;
- доставка;
- размещение и размер производственных подразделений и складов;
- возможности проведения научно-исследовательских работ.

Ш. Информация об организационных особенностях и финансах:

- выявление лиц, принимающих ключевые решения;
- философия лиц, принимающих ключевые решения;
- программы расширения и приобретений;
- главные проблемы и возможности их решения;
- программа проведения научно-исследовательских работ.

Приведенные направления охватывают практически все аспекты дея-

тельности предприятия, фирмы или компании. И пытаться защитить коммерческую тайну, накладывая ограничения на доступ к информации по перечисленным направлениям, вряд ли возможно, но оказывать противодействие соперникам по конкурентной борьбе на рынке просто необходимо. Вот здесь-то аналитические подразделения и должны сыграть свою роль в определении ключевой информации, выявлении возможных каналов утечки, поиске путей ее защиты.

4. ПОРЯДОК УСТАНОВЛЕНИЯ И СНЯТИЯ ГРИФА «КОММЕРЧЕСКАЯ ТАЙНА» НА ПРИЕДПРИЯТИИ

Одним из основополагающих элементов системы мер по обеспечению безопасности информации, составляющей коммерческую тайну предприятия, является выделение документов и изделий, содержащих охраняемые сведения, из общего информационного потока. Выделение таких документов и изделий может осуществляться присвоением им грифа «Коммерческая тайна».

Проставление грифа «Коммерческая тайна» является меткой, которая включает систему защиты охраняемой информации. Поэтому, если система защиты информации функционирует надежно, своевременность установления грифа «Коммерческая тайна» охраняемой информации имеет принципиально важное значение для ее защиты.

Вместе с тем, в соответствии с общепринятым понятием коммерческой тайны, важным является и то обстоятельство, которое позволяет ограничительный гриф по истечении надобности оперативно снимать.

Предлагаемый порядок установления и снятия грифа «Коммерческая тайна» не окажет должного влияния на защиту охраняемой информации вне связи с другими элементами системы.

Порядок установления и снятия грифа «Коммерческая тайна» для различных предприятий, фирм может различаться. Однако, во всех случаях он должен предусматривать следующие аспекты:

кто, когда и как устанавливает гриф «Коммерческая тайна» документу и изделие;

кто, когда и как этот гриф снимает;

права, обязанности и ответственность должностных лиц, устанавливающих и снимающих ограничительный гриф;

контроль за этой сферой деятельности.

При необходимости, можно вводить ограничительные пометки психологического характера. Например, на определенные категории документов, содержащих охраняемые сведения, можно прикреплять ярко выполненные таблички: «На столе не оставлять», «Хранить в сейфе».

4.1. Установление грифа «Коммерческая тайна» документам и изделиям

Гриф «Коммерческая тайна» устанавливается документу или изделию разработчиком этого документа или изделия на стадии подготовки проекта до-

кумента и технической документации на изделие.

При установлении грифа «Коммерческая тайна» разработчик руководствуется требованиями заказчика и Перечнем сведений, составляющих коммерческую тайну предприятия. Сведения, которые должны являться коммерческой тайной, заказчику целесообразно указывать в договоре на проведение этих работ. Причем, заказчику и исполнителю работ необходимо позаботиться о том, чтобы требования заказчика в части сведений, являющихся коммерческой тайной, и Перечень сведений, составляющих коммерческую тайну предприятия-исполнителя в части выполняемой работы, не вступали в противоречие. Сведения, составляющие коммерческую тайну, могут быть указаны и в других документах (ТЗ, ТТЗ), но с соответствующей ссылкой на это обстоятельство в договоре.

На документах гриф «Коммерческая тайна» проставляется на первом (титульном) листе и на обложке в правом углу в соответствии с ГОСТ 6.39-90. На чертежно-конструкторской и технологической документации гриф проставляется в местах, отведенных соответствующими ГОСТами. Если гриф «Коммерческая тайна» устанавливается изделию, то это указывается в сопроводительной документации на изделие (в формуляре, паспорте). При этом в сопроводительной документации необходимо также указать, какая составная часть изделия содержит охраняемые сведения.

Если документы с грифом «Коммерческая тайна» направляются с сопроводительным письмом, то на нем этот гриф также проставляется.

СЛЕДУЕТ ПОМНИТЬ, что научно-техническую, проектно-технологическую и др. документацию, содержащую сведения, составляющие коммерческую тайну, необходимо оформлять таким образом, чтобы сведения, составляющие коммерческую тайну, были максимально локализованы (например, собраны в отдельном томе или разделе документации). Это позволит уменьшить объем документов, что является одним из важных условий обеспечения надлежащей защиты охраняемых сведений.

Приведенные рекомендации устанавливают, в основном, порядок присвоения грифа «Коммерческая тайна» разрабатываемым документам и изделиям. Однако нельзя исключать случаи поступления на предприятие негрифованных документов (изделий), в которых содержатся сведения, составляющие коммерческую тайну предприятия-получателя.

Предприятие-получатель имеет право установить полученным документам (изделиям) гриф «Коммерческая тайна» в соответствии со своим «Перечнем сведений, составляющих коммерческую тайну» в случаях, если:

предприятие-разработчик документа (изделия) было обязано установить гриф «Коммерческая тайна» по условиям договора. Предприятие-разработчик документа (изделия) немедленно уведомляется о допущенном им нарушении договора. Если предприятие, допустившее нарушение, смогло своевременно реализовать необходимые и достаточные меры по защите охраняемой информации от утечки, то инцидент может быть исчерпан. В противном случае во-

прос о возмещении ущерба решается в соответствии с действующим законодательством;

предприятие-разработчик документа (изделия) не связано с предприятием-получателем условиями договора, но по договоренности с предприятием-получателем согласно включить эти сведения в свой «Перечень сведений, составляющих коммерческую тайну» и обеспечить необходимую защиту этой информации. Следует иметь в виду, что без согласия предприятия-разработчика и принятия им соответствующих мер установление грифа «Коммерческая тайна» предприятием-получателем документа (изделия) лишено смысла.

4.2. Снятие грифа «Коммерческая тайна» с документов и изделий

Снятие грифа «Коммерческая тайна» с документа или изделия осуществляет должностное лицо, подписавшее (утвердившее) этот документ или техническую документацию на изделие, или руководитель предприятия.

Основанием для снятия грифа «Коммерческая тайна» с документов и изделий являются:

требования заказчика;

соответствующая корректировка «Перечня сведений, составляющих коммерческую тайну» предприятия;

гриф «Коммерческая тайна» был установлен неправильно;

истечение установленного срока действия грифа.

О снятии грифа «Коммерческая тайна» соответствующее должностное лицо делает отметку на самом документе и в технической (сопроводительной) документации на изделие путем зачеркивания грифа с проставлением своей подписи и даты.

Лица, осуществляющие учет документов (изделий) с грифом «Коммерческая тайна», делают необходимые отметки в соответствующих учетных документах (формах) с указанием фамилии лица, снявшего гриф, и даты снятия.

О снятии грифа «Коммерческая тайна» предприятие, устанавливавшее гриф, извещает все предприятия, связанные договорными обязательствами с предприятием-разработчиком в части охраны коммерческой тайны. Извещение является основанием для снятия грифа «Коммерческая тайна» с полученных документов или изделий. Выполняют эту операцию лица, осуществляющие учет документов или изделий с грифом «Коммерческая тайна».

4.3. Обеспечение правильности определения своевременности установления и снятия грифа «Коммерческая тайна»

Ответственность за правильность определения и своевременность установления и снятия грифа «Коммерческая тайна» несут разработчики этих документов или изделий и руководители, подписавшие (утвердившие) документы или техническую документацию на изделия.

Контроль за правильностью определения и своевременностью установления и снятия грифа «Коммерческая тайна» осуществляют лица, назначенные

руководителем предприятия. Права, обязанности и ответственность этих лиц должны быть определены документально (например, в должностных инструкциях, Положениях и т. п.) и известны сотрудникам предприятия.

5. ОРГАНИЗАЦИЯ И ВЕДЕНИЕ НА ПРЕДПРИЯТИИ ДЕЛОПРОИЗВОДСТВА ДОКУМЕНТОВ С ГРИФОМ «КОММЕРЧЕСКАЯ ТАЙНА».

Настоящие рекомендации позволяют установить обязательные для всех исполнителей требования по учету, размножению, хранению, использованию, отборке на архивное хранение и уничтожение документов с грифом «Коммерческая тайна».

Рекомендации разработаны с учетом положений «Единой государственной системы документированного обеспечения управления» (ЕГСДОУ) и действующих ГОСТов на организационно-распорядительную документацию (ОРД), использованы основополагающие и наиболее эффективные методы и приемы ведения делопроизводства, обеспечивающие надежную сохранность документов и безопасность информации, содержащей коммерческую тайну предприятия.

Организация и ведение делопроизводства документов с грифом «Коммерческая тайна» возлагается на специальное подразделение или на специально назначенных работников предприятия.

Учитывая большой опыт по ведению секретного делопроизводства, а также наличие специально оборудованных помещений и средств, целесообразно поручить ведение делопроизводства документов с грифом «Коммерческая тайна» сотрудникам секретных органов.

В случае, если на предприятии отсутствуют секретные органы, ведение делопроизводства документов с грифом «Коммерческая тайна» возлагается на канцелярию, специально созданное подразделение и на специально назначенных лиц.

Независимо от системы делопроизводства, существующей на предприятии (централизованная, децентрализованная, смешанная), необходимо обеспечить методическое единство в построении учета, прохождения и обращения документов с грифом «Коммерческая тайна».

Структура, штаты и численность подразделений по ведению делопроизводства документов с грифом «Коммерческая тайна» определяются руководителем предприятия в зависимости от объема документооборота, разрабатываются должностные инструкции, в которых необходимо предусмотреть их права, обязанности, ответственность по вопросам сохранения коммерческих секретов.

5.1. Размещение подразделений по ведению делопроизводства с грифом «Коммерческая тайна»

Подразделения по ведению делопроизводства документов с грифом

«Коммерческая тайна» должны размещаться в отдельных, изолированных помещениях, несанкционированный доступ, в которые должен быть исключен.

Документы должны храниться на металлических закрывающихся стеллажах, в металлических шкафах или сейфах. Хранение документов с грифом «Коммерческая тайна» в служебных помещениях других подразделений может осуществляться по разрешению руководителя предприятия при обеспечении условий их надежной сохранности.

В случае размещения подразделений по ведению делопроизводства документов с грифом «Коммерческая тайна» в помещениях секретных органов или канцеляриях должно быть обеспечено отдельное хранение документов с грифом «Коммерческая тайна» от других документов (отдельные комнаты, сейфы, стеллажи).

5.2. Учет документов с грифом «Коммерческая тайна»

Все документы с грифом «Коммерческая тайна», изданные или поступившие на предприятие, подлежат учету в подразделении по ведению делопроизводства документов с грифом «Коммерческая тайна».

Учет документов с грифом «Коммерческая тайна» осуществляется отдельно от учета секретных и несекретных, а также с грифом «Для служебного пользования» документов.

Для решения задач сохранности документов, облегчения справочной работы и обеспечения контроля исполнения целесообразно вести следующие виды учета:

- учет входящих документов;
- учет исходящих (подготовленных) документов;
- инвентарный учет;
- номенклатура дел, журналов, карточек.

Прием и регистрация документов с грифом «Коммерческая тайна» осуществляется подразделением по ведению делопроизводства документов с грифом «Коммерческая тайна». Однократная регистрация распространяется и на документы с грифом «Коммерческая тайна».

Если на предприятии вся получаемая корреспонденция поступает в экспедицию, а также при получении корреспонденции в нерабочее время дежурным по предприятию, пакеты с грифом «Коммерческая тайна» не вскрываются и передаются в подразделение по ведению делопроизводства документов с грифом «Коммерческая тайна».

Ошибочно поступившие документы с грифом «Коммерческая тайна» возвращаются отправителю.

В случае отсутствия (недостачи) в пакетах документов (экземпляров, листов, приложений) с грифом «Коммерческая тайна» составляется акт (приложение № 1) в двух экземплярах, один из которых высылается отправителю.

Регистрация поступивших документов с грифом «Коммерческая тайна» производится на карточках (приложение № 2) или в журналах, которые должны

иметь аналогичные грифы.

Картотеки или журналы учета входящих документов с грифом «Коммерческая тайна» учитываются в номенклатуре. Листы журналов нумеруются, прошиваются и опечатываются.

На первом листе зарегистрированного входящего документа с грифом «Коммерческая тайна» проставляется штамп, в котором указывается наименование предприятия, входящий номер документа, дата регистрации, количество листов основного документа и приложений.

Образец штампа:

Наименование предприятия	
Входящий № и дата	Количество листов основных приложений

На первом листе каждого приложения к входящему документу проставляется штамп с указанием номера входящего документа, приложением к которому является данный документ и количество листов данного приложения.

Образец штампа:

к вх. н	листов

Печатание документов с грифом «Коммерческая тайна» производится в машбюро подразделения по ведению делопроизводства документов с грифом «Коммерческая тайна». По решению руководителя предприятия печатание может быть разрешено в рабочих помещениях исполнителей документов при условии исключения получения охраняемой информации посторонними лицами.

На последнем листе каждого экземпляра отпечатанного документа необходимо проставить количество отпечатанных экземпляров, фамилию исполнителя документа, фамилию машинистки или лица, печатавшего документ и дату.

Отпечатанный документ, а также материалы, подготовленные в рукописном или графическом исполнении, регистрируются в подразделении по ведению делопроизводства документов с грифом «Коммерческая тайна» на карточках (приложение № 3) или в журналах, имеющих соответствующие графы.

Картотеки или журналы учета подготовленных документов с грифом «Коммерческая тайна» учитываются в номенклатуре. Листы журналов нумеруются, прошиваются и опечатываются.

Учетные номера проставляются на первом листе каждого экземпляра документа, а также на последнем листе перед отметкой о количестве отпечатанных экземпляров.

Все черновики, а также варианты и испорченные при печатании листы должны быть сданы в подразделение по ведению делопроизводства документов

с грифом «Коммерческая тайна» для уничтожения.

Инвентарному учету подлежат разработанные на предприятии и присланные из других предприятий научно-технические, чертежно-конструкторские и Другие документы, не подлежащие подшивке в дела. Присланные документы берутся на инвентарный учет после их регистрации по входящему учету и рассмотрения соответствующими должностными лицами.

На инвентарный учет не берутся технические и другие документы, подшиваемые в дела, а также документы, присланные на согласование и во временное пользование.

В зависимости от специфики предприятия, количества документов инвентарный учет может вестись раздельно по наименованиям и видам документов, а также по видам производства.

Инвентарный учет ведется по карточкам (приложение № 4) или журналам, имеющим графы, аналогичные графам карточки. Листы журналов нумеруются, прошиваются и опечатываются. Картотеки или журналы учитываются в номенклатуре.

На инвентарный учет берутся подготовленные подлинники технических документов. Копии учитываются за номером оригинала. Если документ изготавливается машинописным способом и черновик уничтожается сразу после изготовления подлинника, то на инвентарный учет берется подлинник, а в карточке (журнале) учета делается отметка об уничтожении черновика.

На документах, взятых на инвентарный учет, проставляется штамп с указанием инвентарного номера и даты регистрации.

Образец штампа:

Инв. н “____” _____ 2000 г.

Штамп с инвентарным номером проставляется:

на сброшюрованных документах - в верхнем левом углу обложки и титульного (первого) листа документа;

на документах, хранящихся россыпью - в верхнем левом углу каждого листа;

на графических документах - над основной надписью.

Дела, журналы, картотеки с грифом «Коммерческая тайна» учитываются по общей номенклатуре дел предприятия.

В графе 1 номенклатуры под индексом, присвоенным данному делу, журналу, картотеке, проставляется гриф «Коммерческая тайна». После графы «Заголовок дела» вводится графа «Фамилии исполнителей, которым предоставлено право пользования делом».

Для подразделения по ведению делопроизводства документов с грифом «Коммерческая тайна» делается выписка из номенклатуры, в которую вносятся все дела, журналы и картотеки с грифом «Коммерческая тайна».

При составлении номенклатуры дел, включающей дела с грифом «Ком-

мерческая тайна», кроме учета требований общего делопроизводства о порядке комплектования дел в соответствии с различными признаками классификации необходимо предусмотреть круг лиц, имеющих право пользоваться делом, не допуская необоснованного его расширения, но и не затрудняя решение производственных вопросов.

Документы с грифом «Коммерческая тайна» подшиваются в дела в соответствии с выпиской из номенклатуры после их исполнения. Все дела с грифом «Коммерческая тайна» независимо от сроков их хранения должны иметь внутреннюю опись, которая выполняет функцию учета документов внутри каждого дела.

Листы дела нумеруются, после закрытия дела прошиваются и опечатываются. Заверительный лист подписывается сотрудником подразделения по ведению делопроизводства документов с грифом «Коммерческая тайна».

5. 3. Отправка документов с грифом «Коммерческая тайна»

Отправка документов с грифом «Коммерческая тайна», во внешние организации осуществляется по разрешению лиц, которым даны на это соответствующие полномочия руководителем предприятия.

Документы отправляются заказными или ценными письмами и заказными бандеролями. По согласованию с соответствующими органами целесообразно использовать каналы специальной связи.

При отправке документов заказными или ценными отправлениями не рекомендуется проставлять на конвертах (пакетах) гриф «Коммерческая тайна», так как это может привлечь внимание посторонних лиц и привести к утечке (хищению) охраняемой информации. В таких случаях рекомендуется использовать двойной конверт. На внутреннем конверте указывать гриф «Коммерческая тайна» и номера документов, а на внешнем - адрес получателя.

Исходящим номером документа с грифом «Коммерческая тайна» является номер, за которым зарегистрирован документ. Например: документ, зарегистрированный по входящему учету, отправляется во внешнюю организацию за своим входящим номером. Документ, стоящий на инвентарном учете, в случае, если он отправляется без сопроводительного письма, отправляется за своим инвентарным номером. Исходящим номером документа, зарегистрированного по учету подготовленных документов, будет этот номер.

После отправки документа в карточке (журнале) учета, по которому зарегистрирован отправляемый документ, делается отметка об отправке, заверяемая подписью лица, производившего отправку.

При необходимости документы с грифом «Коммерческая тайна» могут доставляться адресату нарочными из числа сотрудников, допущенных к работе с такими документами.

5.4. Уничтожение документов с грифом «Комическая тайна»

Уничтожение документов с грифом «Коммерческая тайна», в том числе

черновиков, бракованных листов и испорченных копий, должно производиться подразделением по ведению делопроизводства документов с грифом «Коммерческая тайна» с обязательной простановкой отметок: об уничтожении в учетных данных документов.

Порядок уничтожения черновиков, испорченных листов, неподписанных проектов документов с грифом «Коммерческая тайна».

Сданные в подразделение по ведению делопроизводства документов с грифом «Коммерческая тайна» черновики, испорченные листы, варианты и неподписанные проекты документов надрываются и помещаются в опечатанную урну (мешок, ящик, портфель). В учетных данных документа (карточке, журнале) делается отметка об уничтожении черновика с указанием количества листов и проставлением подписи сотрудника подразделения по ведению делопроизводства с грифов «Коммерческая тайна» и даты.

По мере накопления содержимое урны (мешка, ящика, портфеля) изымается работниками подразделения по ведению делопроизводства документов с грифом «Коммерческая тайна» и уничтожается. Периодичность изъятия может устанавливаться начальником подразделения по ведению делопроизводства документов с грифом «Коммерческая тайна» в зависимости от количества документов и условий уничтожения.

Уничтожение документов с грифом «Коммерческая тайна» производится в соответствии со сроками и в порядке, определяемом Главным архивным управлением РФ или ведомством.

Разрешение на уничтожение дает руководитель подразделения, к деятельности которого относится документ, путем проставления в учетной карточке (журнале) резолюции «Уничтожить», своей подписи и даты.

При проведении экспертизы ценности документов перед их передачей на архивное хранение, отбор документов на уничтожение производит экспертная комиссия.

Отобранные для уничтожения документы и дела с грифом «Коммерческая тайна» вносятся в акт установленной формы, сверяются перед уничтожением работниками подразделения по ведению делопроизводства документов с грифом «Коммерческая тайна» с учетными данными и уничтожаются.

После уничтожения в учетных данных производятся отметки с указанием номера акта, даты уничтожения и подписи сотрудников, производивших уничтожение.

Уничтожение документов и дел с грифом «Коммерческая тайна» должно производиться путем их сожжения или измельчения или другим путем, исключающим восстановление текста документов.

5.5. Проверка наличия документов с грифом «Коммерческая тайна»

Периодические проверки наличия документов с грифом «Коммерческая тайна» являются важным фактором, обеспечивающим их физическую сохранность.

В ходе проверок устанавливается соответствие наличия документов учетных данных, правильность ведения учетов, проверяется порядок обращения с документами, рассматриваются вопросы снятия грифа «Коммерческая тайна».

Проверки проводятся комиссионно, с обязательным включением в комиссию работников, ответственных за учет и хранение документов с грифом «Коммерческая тайна».

Проверки осуществляются от учетных данных к документам, проверяется наличие всех зарегистрированных экземпляров. Документы, хранящиеся россыпью, проверяются полистно. В ходе проверок устанавливается соответствие и правильность заполнения граф учетных карточек и журналов, наличие отметок об отправке, возврате, размножении и уничтожении документов.

Рекомендуется проводить ежеквартальные и ежегодные проверки наличия документов с грифом «Коммерческая тайна».

Квартальная проверка наличия проводится в первую декаду первого месяца, следующего за последним месяцем проверяемого квартала.

В квартальную проверку проверяются документы, находящиеся на исполнении, не подшитые в дела и не взятые на инвентарный учет, а также документы, находящиеся на хранении в подразделениях или на руках у исполнителей.

Годовая проверка наличия проводится в январе следующего за проверяемым года.

В годовую проверку проверяется наличие всех зарегистрированных документов с грифом «Коммерческая тайна», а также правильность ведения всех видов учета и порядка оформления актов на уничтожение.

Проверки наличия документов проводятся также при смене руководителя подразделения по ведению делопроизводства документов с грифом «Коммерческая тайна» или сотрудников этих подразделений, ответственных за учет и хранение документов.

Результаты проверок оформляются актами. Акты подписывают члены комиссии по проверке наличия документов и утверждают у руководителя предприятия.

5.6. Порядок хранения и обращения с документами с грифом «Коммерческая тайна»

Документы с грифом «Коммерческая тайна» в нерабочее время должны храниться в помещениях подразделений по ведению делопроизводства документов с грифом «Коммерческая тайна». Хранение документов в нерабочее время в других помещениях допускается по решению руководителя предприятия при наличии условий, обеспечивающих их сохранность.

Выдача документов с грифом «Коммерческая тайна» сотрудникам предприятия, а также сотрудникам других предприятий и учреждений производится только по разрешению должностных лиц в соответствии с действующей на предприятии разрешительной системой под роспись в карточке учета выдачи документа или дела (приложение № 5), или в учетной карточке документа.

Передача документов с грифом «Коммерческая тайна» между сотрудниками предприятия может осуществляться только под расписку и в пределах круга лиц, допущенных к данному документу в соответствии с действующей на предприятии разрешительной системой (приложение № 6).

При работе с документами с грифом «Коммерческая тайна» сотрудникам предприятия следует помнить о своих обязательствах по неразглашению охраняемых сведений и выполнению на предприятии правил обращения с грифованной информацией принимать необходимые разумные меры, исключающие утрату документов или утечку коммерческих секретов.

6. ПОЛУЧЕНИЯ РАЗРЕШЕНИЙ НА ДОСТУП К ИНФОРМАЦИИ, ЯВЛЯЮЩЕЙСЯ КОММЕРЧЕСКОЙ ТАЙНОЙ НА ПРЕДПРИЯТИИ

Одним из ключевых звеньев в обеспечении защиты информации от несанкционированного доступа к ней является СИСТЕМА ПОЛУЧЕНИЯ РАЗРЕШЕНИЙ НА ДОСТУП К ОХРАНЯЕМОЙ ИНФОРМАЦИИ (в дальнейшем для краткости – «Разрешительная система»).

При разработке такой системы применительно к сведениям, составляющим коммерческую тайну, должны быть проработаны и четко сформулированы следующие вопросы:

кто на предприятии имеет право давать разрешение на доступ и к каким сведениям;

кому и при каких условиях разрешение на доступ к сведениям, составляющим коммерческую тайну, может быть дано.

Необходимо отметить, что делопроизводческие процедуры, которые также влияют на обеспечение сохранности информации, отличаются в зависимости от вида носителя информации (бумага, изделия, магнитные носители) и вида документа (приказы, отчеты, номенклатурные дела). Кроме того, вид документа связан с важностью помещаемой в нем информации (техническое задание, технический проект, приказ, отчет).

Эти обстоятельства тоже должны учитываться при разработке Разрешительной системы.

Следует также тщательно проработать процедурные вопросы, связанные с доступом к охраняемой информации представителей других предприятий. Здесь необходимо уделить должное внимание тому, чтобы характер и объем информации, с которой будет разрешено ознакомить представителя другого предприятия, точно соответствовал его полномочиям, а также взаимным обязательствам предприятий по защите сведений, являющихся коммерческой тайной. Речь идет, в том числе, и об информации, которая может быть получена вербально.

В связи с возможностью несанкционированного получения охраняемой информации вербальным путем при проведении переговоров и совещаний в Раз-

решительной системе следует отразить также требования, касающиеся защиты коммерческой тайны при проведении таких мероприятий.

Применение мер защиты сведений, составляющих коммерческую тайну предприятия, неизбежно приводит к усложнениям в обращении с такой информацией. Это вызывает определенный дискомфорт у пользователей охраняемой информации. Но если на предприятии принято решение о необходимости НАДЕЖНОЙ ЗАЩИТЫ ИНФОРМАЦИИ, составляющей его коммерческую тайну, то Разрешительная система, разработанная по настоящим рекомендациям, в значительной степени поможет это сделать при минимально необходимых ограничениях для пользователей.

Необходимо отметить, что полнота применения рекомендаций в большой мере зависит от структуры предприятия, характера его деятельности и объема документов с грифом «Коммерческая тайна». В самом простом случае (небольшое предприятие, серийное производство, незначительный объем грифованных документов) разрешение на доступ к охраняемой информации может, например, давать только руководитель предприятия. Если же предприятие является многоцелевым, с разветвленной производственной и административной структурой и значительным документооборотом, то выдача разрешений на доступ к охраняемой информации только руководителем предприятия скорее всего приведет или к дезорганизации производства, или к компрометации всей системы защиты охраняемой информации действующей на предприятии.

6.1. Структура системы получения разрешения на доступ к информации, являющейся коммерческой тайной предприятия

С учетом многолетнего опыта защиты охраняемой информации в ряде отраслей народного хозяйства, а также соображений, изложенных в предыдущем разделе Рекомендаций, «Система получения разрешений на доступ к информации, являющейся коммерческой тайной предприятия» должна содержать следующие разделы: общие положения;

права, обязанности и. ответственность сотрудников предприятия в пределах Разрешительной системы;

схема выдачи разрешений на доступ сотрудников ; предприятия к сведениям, составляющим коммерческую тайну;

порядок оформления разрешений на доступ к сведениям, составляющим коммерческую тайну предприятия;

рассылка грифованных документов в другие предприятия и передача между подразделениями предприятия;

порядок доступа на совещания по вопросам, содержащим сведения, являющиеся коммерческой тайной;

порядок доступа к сведениям, составляющим коммерческую тайну, представителей других предприятий и государственных органов.

Разрешительная система - это совокупность правил, регулирующих порядок доступа работников предприятия и других лиц к сведениям (работам, доку-

ментам изделиям), являющимся коммерческой тайной.

Целями введения Разрешительной системы на предприятии являются:

- исключение несанкционированного или необоснованного ознакомления со сведениями, являющимися коммерческой тайной;

- своевременное обеспечение требующейся грифованной информацией исполнителей работ и документов.

Разрешение на доступ работника предприятия к сведениям, являющимся коммерческой тайной, может быть дано соответствующими должностными лицами предприятия только при выполнении следующих условий:

- наличии приказа руководителя предприятия о приеме на работу (переводе, временном замещении) или назначении на должность;

- при временном замещении отсутствующего работника его должностные обязанности допускается возлагать на исполнителя, имеющего прямое отношение к выполняемой работе;

- оформлении обязательства о сохранении им сведений составляющих коммерческую тайну;

- изучении вновь принятым работником (назначенным на должность) требований нормативных документов обеспечению сохранности коммерческой тайны. После изучения нормативных требований по сохранению охраняемых сведений руководитель подразделения, где такие сведения имеются, с вновь принятым (назначенным на должность) работником проводит собеседование. Результаты собеседования оформляются в журнале.

Работники предприятия могут получать разрешение на доступ к сведениям, составляющим коммерческую тайну, только в пределах своих должностных (функциональных) обязанностей и в объемах, действительно необходимых им для выполнения служебных обязанностей.

Руководители предприятия и его подразделений несут персональную ответственность за правомерность выдаваемых ими разрешений на доступ исполнителей к сведениям, составляющим коммерческую тайну.

Контроль за соблюдением требований разрешительной системы возлагается на руководителя подразделения, которое ведет делопроизводство документов с грифом «Коммерческая тайна».

6.1.1. Права, обязанности и ответственность работников предприятия в пределах «Разрешительной системы»

Права, обязанности и ответственность руководителей подразделений предприятия.

Руководители подразделений имеют право:

давать разрешения на доступ к сведениям, составляющим коммерческую тайну, своим подчиненным и переадресовывать руководителям подразделений-соисполнителей работ;

отменять неправомерное адресование документов исполнителям руководителями подчиненных подразделений;

принимать меры к подчиненным сотрудникам, допускающим нарушения требований Разрешительной системы, в пределах предоставленных им прав;

поощрять работников своего подразделения, проявляющих инициативу в пресечении нарушений требований Разрешительной системы.

Руководители подразделений обязаны:

исполнять требования Разрешительной системы лично и обеспечивать его исполнение подчиненными сотрудниками;

осуществлять контроль за выполнением требований Разрешительной системы в своём подразделении;

пресекать действия подчиненных, ведущие к нарушениям требований Разрешительной системы;

не допускать неоправданного расширения доступа к охраняемым сведениям и принимать меры к исключению неправомерного ознакомления сотрудников с грифованной информацией; вести воспитательную и разъяснительную работу среди подчиненных по предупреждению утечки сведений, составляющих коммерческую тайну, при работе с грифованными документами и изделиями.

Руководители подразделений несут ответственность;

за нарушение требований Разрешительной системы ими лично и подчиненными сотрудниками.

Исполнители имеют право:

требовать от руководителей создания необходимых условий для работы с грифованными документами;

вносить предложения по совершенствованию Разрешительной системы.

Исполнители обязаны знать и выполнять требования Разрешительной системы.

Исполнители несут личную ответственность за соблюдение ими требований Разрешительной системы.

Сотрудники подразделений, осуществляющие делопроизводство документов с грифом «Коммерческая тайна» имеют право и обязаны:

требовать от всех сотрудников предприятия точного и неукоснительного выполнения требований Разрешительной системы;

вносить предложения по совершенствованию Разрешительной системы и наказания лиц, допустивших нарушения ее требований;

осуществлять контроль за соблюдением требований разрешительной системы;

не допускать неправомерного ознакомления с грифованными документами;

докладывать своему руководителю о фактах нарушений требований Разрешительной системы и других действиях, могущих привести к утечке сведений, составляющих коммерческую тайну, или утрате грифованных документов.

Несут ответственность за неиспользование своих прав и неисполнение

обязанностей в рамках Разрешительной системы.

6.1.2. Схема выдачи разрешений на доступ сотрудников предприятия к сведениям, составляющим коммерческую тайну

Схема выдачи разрешений на доступ сотрудников предприятия к охраняемой информации является ключевым элементом, определяющим эффективность Разрешительной системы в целом.

Поэтому, при разработке «Схемы...» необходимо в полной мере учитывать структуру предприятия, сложившуюся систему управления, производственные связи внутри предприятия, распределение обязанностей между заместителями руководителя предприятия и т. д. Следует также иметь в виду, что чрезмерные ограничения в выдаче разрешений на доступ к охраняемой информации неизбежно приведут к снижению оперативности в решении производственных вопросов, в то время как излишняя либерализация создаст условия для утечки сведений, составляющих коммерческую тайну предприятия.

Выдача разрешения на доступ сотрудников предприятия к сведениям, составляющим коммерческую тайну, будет полной и удобной в работе, если проработать и изложить ее в 2-х аспектах:

выдача разрешений в зависимости от категорий документов;

выдача разрешений в зависимости от занимаемой должности.

Схема выдачи разрешений в зависимости от категории документов.

Целесообразно выделить следующие категории документов:

номенклатурные дела;

документы входящего учета;

документы подразделений;

документы, находящиеся на архивном хранении в подразделении фондов НТД предприятия;

носители информации средств ЭВТ.

При необходимости можно выделить также другие категории документов. Например, документы, отражающие взаимоотношения с собственником, с финансирующими организациями (Министерство, банки), материалы информационного обмена и т. п.

При этом «Схема...» будет выглядеть следующим образом:

Категории документов	Должностное лицо, дающее разрешение	Категории сотрудников, кому дается разрешение
1	2	3
Например: Номенклатурные дела	Руководитель предприятия при утверждении номенклатуры, подписанной руководителем подразделения делопроизводства документов с грифом «Коммерческая тайна».	Сотрудникам института

1	2	3
Документы подразделений	Руководитель предприятия, его заместители	Сотрудникам института
	Руководители подразделений	Своим подчиненным, руководителям подразделений-соисполнителей работ, руководителям работ

Схема выдачи разрешений в зависимости от занимаемой должности.

В этом случае схема будет выглядеть следующим образом:

Должность	Категории документов, на ознакомление с которыми имеет право давать разрешение	Категории сотрудников, кому дается разрешение
Например: Руководитель предприятия Руководители подразделений	Все документы, находящиеся на предприятии Документы подразделений	Сотрудникам предприятия Своим подчиненным, руководителям подразделений соисполнителей работ, руководителям работ
Помощник руководи- теля предприятия по между- народным связям	Все документы по вопросам международного сотрудничества	Сотрудникам предприятия

Правомерно выделить категории сотрудников предприятия, которые имеют право знакомиться с грифованными документами без дополнительного разрешения. Однако, при этом надо определить, о каких документах идет речь. Например:

Заместители руководителя предприятия	со всеми документами по своим направлениям деятельности.
Руководители подразделений	со всеми документами, изданными или поступившими в подчиненные им подразделения (кроме случаев, оговариваемых особо).
Руководитель подразделения фондов НТД	со всеми документами, кроме документов с пометкой

	«Лично»
Сотрудники подразделения фондов НТД	в пределах списков, подписанных руководителем подразделения и утвержденных руководителем предприятия.
Главный бухгалтер предприятия	со всеми документами, касающимися финансовой деятельности предприятия.
Исполнитель документа	со всеми исполненными им документами на период действия его обязательств в части сохранения коммерческой тайны предприятия.

6.1.3. Порядок оформления разрешения на доступ к сведениям, составляющим коммерческую тайну предприятия

Разрешения на доступ к документам с грифом «Коммерческая тайна» даются только в письменном виде: на карточках разрешений, на списках ознакомления, на самих документах или в форме приказов (указаний).

В случае, когда исполнитель допускается только к части документа, в разрешении должны четко указываться конкретные пункты, разделы, части или страницы, к которым допускается исполнитель, а сотрудники подразделения по ведению делопроизводства документов с грифом «Коммерческая тайна» принимают необходимые меры, исключающие ознакомление с другими частями документа.

Порядок оформления разрешений на доступ к номенклатурным делам.

В соответствии с номенклатурой дел для каждого тома на внутренней стороне обложки или на карточке-разрешении составляется список сотрудников, допущенных к документам, подшитым в дело. Список заверяется подписью сотрудника подразделения по ведению делопроизводства документов с грифом «Коммерческая тайна».

Ознакомление сотрудников предприятия с отдельными документами в деле производится по письменному разрешению соответствующего руководителя. При этом сотрудниками подразделения по ведению делопроизводства документов с грифом «Коммерческая тайна» должны быть приняты меры, исключающие ознакомление исполнителя с другими документами, подшитыми в дело.

Изменения и дополнения в списки лиц, допущенных номенклатурным делам, вносит руководитель подразделения по ведению делопроизводства с грифом «Коммерческая тайна» по письменному представлению руководителя соответствующего подразделения.

Разрешение на доступ к документам входящего учета дается на самом документе в виде резолюции соответствующего руководителя.

Разрешения на доступ к документам подразделений могут даваться в любых формах предусмотренных в инструкциях.

Доступ исполнителей к документам с грифом «Коммерческая тайна», находящимся на архивном хранении в подразделении фондов НТД осуществляется по требованиям установленного образца.

Требование подписывает руководитель подразделения, где работает исполнитель, которому нужен документ, и согласовывает руководитель подразделения фондов НТД.

Чтобы исключить неправомерное получение исполнителем документа с охраняемыми сведениями, из заполненного требования должно быть ясно, какой документ запрашивается.

Если исполнителю необходимо ознакомиться только с частью дела или документа, то об этом делается отметка в требовании и сотрудники подразделения фондов НТД принимают необходимые меры, исключающие ознакомление с другими частями дела или документа.

Выдача документов с грифом «Коммерческая тайна» авторам, а также исполнителям, которые ранее .пользовались ими, производится по требованиям, подписанным руководителем подразделения. Согласующая подпись руководителя подразделения фондов НТД не требуется. Подпись руководителя подразделения означает, что тематика работы исполнителя не изменилась.

Без оформления требований доступ к документам с грифом «Коммерческая тайна» могут иметь: (указываются должности и категории документов. Например: руководитель предприятия - ко всем документам; руководитель подразделений - к документам, созданным в деятельности подчиненных им подразделений; и т. д.)

Отправка документов с грифом «Коммерческая тайна» из фонда предприятия в другие предприятия во временное пользование производится с разрешения руководителя предприятия или его заместителя.

6.1.4. Рассылка документов с грифом «Коммерческая тайна» в другие предприятия передача между подразделениями предприятия

Устанавливая полномочия должностных лиц предприятия по данному разделу, не следует забывать, что после отправки документа предприятие практически теряет над ним контроль. Поэтому минимизация круга должностных лиц, имеющих право давать разрешение на отправку документа с грифом «Коммерческая тайна», а также круга предприятий, куда такие документы могут направляться, существенно поможет обеспечить защиту охраняемой информации от утечки.

Причем объем и содержание охраняемой информации, включенной в документы, направляемые в другие предприятия, должны соответствовать условиям договоров или специализации и информационной потребности этих предприятий, если договора отсутствуют.

Документы с грифом «Коммерческая тайна» разрешается направлять...

(Указывается куда. Например: Заказчику, в Министерство, ГНТУ и т. д.).

Грифованные документы направляются в другие предприятия по разрешению. (Указывается перечень должностей. Например: руководитель предприятия, его заместители и т.д.).

Право ведения переписки с грифом «Коммерческая тайна» также предоставляется (Если есть необходимость в этом пункте, то нужно указать должности и по каким вопросам. Например: начальнику патентного отдела - по вопросам изобретательства и рационализации; и т.д.).

Отправка документов производится по сопроводительным письмам, спискам рассылки или разрешениям, оформленным в учетных формах.

Необходимость отправки, объем грифованной информации и срок, на который производится отправка, определяются лицом, подписывающим документ на отправку и должны быть обоснованы.

Исходящая документация с грифом «Коммерческая тайна» контролируется руководителем подразделения по ведению делопроизводства документов с грифом «Коммерческая тайна» с целью проверки правильности оформления документов согласно требованиям делопроизводства документов с грифом «Коммерческая тайна».

Передача документов с грифом «Коммерческая тайна» между подразделениями предприятия производится по разрешению начальника подразделения.

Пересылка номенклатурных дел с грифом «Коммерческая тайна» между подразделениями предприятия осуществляется по совместному разрешению руководителя подразделения (работ) и руководителя подразделения по ведению делопроизводства документов с грифом «Коммерческая тайна».

6.1.5. Порядок доступа на совещание по вопросам, содержащим сведения, являющиеся «Коммерческой тайной»

Разрешение на проведение совещаний могут давать руководитель предприятия, его заместители, руководители подразделений, руководители работ. В этой связи необходимо установить и отразить в Разрешительной системе уровень полномочий каждого руководителя.

Руководитель, давший разрешение на проведение совещания, назначает ответственного за его проведение. Ответственный за проведение совещания составляет список его участников и утверждает у руководителя, давшего разрешение на проведение.

В случае, если сотрудник предприятия или представитель другого предприятия приглашаются для обсуждения отдельного вопроса повестки, то об этом делается отметка в списке.

На совещание пропускаются только те лица, которые значатся в списке.

К участию в совещании должны привлекаться только те работники предприятия и представители других предприятий, которые ведут работы по обсуждаемым вопросам и имеют к ним непосредственное отношение.

Целесообразно, чтобы руководитель, открывая совещание, напомнил

участникам о необходимости сохранения коммерческой тайны, а также уточнил, какие конкретно сведения являются охраняемыми.

Необходимо также позаботиться, чтобы в ходе совещания охраняемая информация не могла быть получена из-за пределов помещения, в котором проводится совещание. Речь идет о возможности применения визуально-оптических, акустических и др. технических средств, которые могут быть установлены заинтересованными лицами как в самом помещении, так и за его пределами.

Ответственность за соблюдение требований по защите коммерческой тайны правомерно возложить на руководителя, организовавшего совещание.

6.1.6. Порядок доступа к сведениям, «Коммерческую тайну», представителей других предприятий и государственных органов

Разрешение на доступ к сведениям, составляющим коммерческую тайну, представителей других предприятий имеют право давать должностные лица в соответствии со списком, утвержденным руководителем предприятия.

При подготовке такого списка целесообразно учитывать структуру предприятия, сложившуюся частоту приема командированных лиц в тех или иных подразделениях, важность совместных работ для данного предприятия. Пересмотр списка рекомендуется производить ежегодно.

НЕОБХОДИМО ПОМНИТЬ, ЧТО РАСШИРЕНИЕ КРУГА ДОЛЖНОСТНЫХ ЛИП, ИМЕЮЩИХ ПРАВО ДАВАТЬ РАЗРЕШЕНИЕ НА ДОСТУП К СВЕДЕНИЯМ, СОСТАВЛЯЮЩИМ КОММЕРЧЕСКУЮ ТАЙНУ, ВМЕСТЕ С УВЕЛИЧЕНИЕМ ОПЕРАТИВНОСТИ В РАБОТЕ УВЕЛИЧИВАЕТ ВЕРОЯТНОСТЬ УТЕЧКИ ОХРАНЯЕМОЙ ИНФОРМАЦИИ

Разрешение на доступ к охраняемым сведениям дается в предписании на выполнение задания с указанием конкретных сведений и (или) номеров грифованных документов, с которыми необходимо ознакомить представителя другого предприятия. При этом должностному лицу, дающему разрешение, должны быть ясны полномочия представителя другого предприятия и объем охраняемых сведений, необходимых ему для выполнения задания.

При выдаче разрешения на доступ к охраняемым сведениям необходимо также указать фамилию работника предприятия, которому поручается ознакомить представителя другого предприятия с указанными сведениями (документами).

Что касается представителей государственных органов, то целесообразно, чтобы разрешение на доступ их к сведениям, составляющим коммерческую тайну, выдавали только руководитель предприятия или его заместитель.

7. ПОРЯДОК УЧЕТА, ХРАНЕНИЯ И ОБРАЩЕНИЯ ИЗДЕЛИЙ С ГРИФОМ «КОММЕРЧЕСКАЯ ТАЙНА» НА ПРЕДПРИЯТИИ

Изделия с грифом «Коммерческая тайна», как и любые другие изделия, являются материальной ценностью предприятия. Уже в этой связи должны быть обеспечены надлежащий учет и физическая сохранность таких изделий. Однако, поскольку изделия с грифом «Коммерческая тайна» являются еще и носителями ОХРАНЯЕМОЙ информации, становится важным не только надежное обеспечение их физической сохранности, но и надежная защита охраняемых сведений, носителями которых изделия являются. Следует помнить, что для сохранения от утечки сведений, составляющих коммерческую тайну, носителями которых является изделие, необходимым условием должно быть принятие эффективных мер по предотвращению:

хищения или утраты изделия;

доступа к изделию посторонних лиц (т.е лиц, которые НЕ ДОЛЖНЫ знать охраняемые сведения);

получения охраняемых сведений при помощи технических средств.

Требующиеся меры могут быть реализованы посредством соответствующей подготовки помещений, предназначенных для разработки, изготовления или хранения изделий с грифом «Коммерческая тайна», а также установления специальных процедур учета, получения, отправки и контроля наличия таких изделий.

7.1. Учет изделий с грифом «Коммерческая тайна»

Все изделия с грифом «Коммерческая тайна», изготавливаемые или полученные предприятием, должны быть взяты на баланс и учтены в бухгалтерии этого предприятия, а также состоять на строгом оперативном учете. На всех стадиях производства, хранения, транспортировки и работы с грифованными изделиями в подразделениях предприятия должна быть установлена персональная ответственность за сохранность этих изделий в любой момент времени.

Изделия с грифом «Коммерческая тайна» берутся на учет:

в опытном производстве - при отсутствии оформленной технологической документации - с момента изготовления их по чертежам с грифом «Коммерческая тайна» или со стадии изготовления, указанной в технических условиях разработчика;

в серийном производстве - с момента, указанного в технологической документации или сопроводительных картах (паспортах), в которых должна быть предусмотрена операция постановки на учет;

полученные из других организаций - с момента поступления учетно-технической документации на них от поставщика.

На каждое изделие с грифом «Коммерческая тайна», изготовленное на предприятии, оформляется паспорт или формуляр, на которых также проставляется этот гриф.

НЕ СЛЕДУЕТ НАЧИНАТЬ ИЗГОТОВЛЕНИЕ ИЗДЕЛИЯ С ГРИФОМ «КОММЕРЧЕСКАЯ ТАЙНА», ЕСЛИ ИСПОЛНИТЕЛЯМ НЕ ЯСНО, С КАКОГО МОМЕНТА ИЗДЕЛИЕ СТАНОВИТСЯ НОСИТЕЛЕМ ОХРАНЯЕМОЙ ИНФОРМАЦИИ

Грифованные изделия учитываются по заводским и инвентарным номерам. Изделия, на которых проставить инвентарный или заводской номер не представляется возможным, следует учитывать по количеству или весу и хранить в отдельной упаковке, на которой проставляется номер».

При нумерации изделий следует помнить, что и общее количество выпущенных изделий может являться коммерческой тайной предприятия.

Для организации надлежащего учета изделий с грифом «Коммерческая тайна» и обеспечения персональной ответственности за их сохранность необходимо сделать еще несколько простых вещей:

назначить лицо, осуществляющее учет грифованных изделий в бухгалтерии предприятия;

в каждом подразделении предприятия, имеющем дело с грифованным изделием, назначить лиц, ответственных за их оперативный учет и сохранность (уполномоченных).

Назначения должны производиться приказом по предприятию. Должны быть также четко определены обязанности, права и ответственность этих лиц.

Передача изделий с грифом «Коммерческая тайна» из одного подразделения предприятия в другое осуществляется через уполномоченных с надлежащим оформлением требования или акта.

7.2. Получение и отправка изделий с грифом «Коммерческая тайна»

Порядок получения и отправки изделий с грифом «Коммерческая тайна» на предприятии существенным образом зависит от 2-х факторов:

частоты получения (отправки) изделий предприятием;

количества структурных подразделений предприятия, которым необходимо получать (отправлять) изделия по условиям договоров с другими предприятиями.

Если частота получения (отправки) изделий небольшая, а круг подразделений-получателей (отправителей) невелик и стабилен, то функции получения (отправки) грифованных изделий могут быть поручены этим структурным подразделениям предприятия.

В противном случае на предприятии необходимо создать специальную группу для обеспечения централизованного получения (отправки) изделий с грифом «Коммерческая тайна», наделив ее необходимыми полномочиями и соответствующим образом оборудованным помещением для хранения грифованных изделий (центральный склад изделий с грифом «Коммерческая тайна»).

Однако, многолетняя практика обращения с изделиями, являющимися носителями охраняемой информации, показала, что ТОЛЬКО ПРИ ЦЕНТРАЛИЗОВАННОМ ПОЛУЧЕНИИ (ОТПРАВКЕ) изделий можно обеспечить их

надлежащий учет и избежать ошибок, способствующих утрате или хищению изделий, а также утечке охраняемой информации.

Исходя из этого, при получении или отправке изделий с грифом «Коммерческая тайна» рекомендуется применять процедуры, изложенные ниже.

От внешних организаций грифованные изделия поступают на Центральный склад.

Приемка грифованных изделий производится по сопроводительной накладной с обязательной проверкой целостности пломб и упаковок, количество которых указано в сопроводительной документации.

Полученное изделие регистрируется в учетном журнале спецгруппы. По получении изделия с грифом «Коммерческая тайна» и сопроводительной документации, сотрудник спецгруппы уведомляет об этом подразделение-получатель, которое обязано в установленные сроки оформить акт передачи и получить изделие, сделав соответствующую запись в учетном журнале спецгруппы.

Вскрытие и проверка изделия в подразделении-получателе производится в присутствии уполномоченного.

В случае несоответствия содержимого упаковки, в которой находится грифованное изделие, данным сопроводительной документации или обнаружения брака составляется акт и делается представление организации-поставщику.

Предназначенные к отправке в другие организации изделия упаковываются подразделением-отправителем при наличии паспорта (формуляра) и упаковочной ведомости на данные изделия и передаются в спецгруппу для отправки.

Отправка грифованных изделий во внешние организации производится спецгруппой на основании «Поручения», подписанного директором предприятия и согласованного с Главным бухгалтером. «Поручение» оформляется подразделением-отправителем.

Отправка и вывоз изделий с грифом «Коммерческая тайна» производится ТОЛЬКО по пропускам спецгруппы.

Внимательно изучив предлагаемый механизм получения и отправки изделий с грифом «Коммерческая тайна», можно отметить, что централизованное оформление процедур получения и отправки грифованных изделий может обеспечить требующийся учет этих изделий и надлежащий контроль за их перемещением.

По-видимому, могут быть предложены и другие варианты, зависящие от конкретных особенностей предприятия. Но во всех случаях должно соблюдаться ГЛАВНОЕ УСЛОВИЕ: лицо (лица), осуществляющее учет и отправку грифованных изделий, должно быть официально назначено приказом по предприятию.

7.3. Транспортировка изделий с грифом «Коммерческая тайна»

Транспортировка изделия должна рассматриваться как операция, связан-

ная с повышенным риском его хищения или утраты. Поэтому транспортировку изделия на другое предприятие следует осуществлять только в случаях КРАЙНЕЙ НЕОБХОДИМОСТИ, причем основные условия транспортировки необходимо изложить в договоре (кто транспортирует изделие; вид транспорта; обеспечение охраны; транспортировка изделия в сборе или по частям; как будет осуществляться возврат изделия, если это необходимо).

Бели по каким-либо причинам условия транспортировки изделий с грифом «Коммерческая тайна» не оговорены, можно руководствоваться следующими рекомендациями.

Отправку изделий в адрес внешних организаций поручать подразделениям, связанным договорными обязательствами с предприятиями, которым изделия необходимо доставить.

Охрану (сопровождение) груза также поручать сотрудникам этих подразделений, соответствующим образом их проинструктировав.

При транспортировке изделия с грифом «Коммерческая тайна» должны быть упакованы так, чтобы исключить их обозрение. Должны быть выбраны наиболее удобный (безопасный) маршрут и время перевозки.

ЕСЛИ ПРЕДСТАВЛЯЕТСЯ ВОЗМОЖНЫМ ИЗЪЯТЬ ИЗ ИЗДЕЛИЯ НОСИТЕЛЬ ОХРАНЯЕМЫХ СВЕДЕНИЙ И УПРОСТИТЬ ПРОБЛЕМЫ, СВЯЗАННЫЕ С ТРАНСПОРТИРОВКОЙ ГРИФОВАННОГО ИЗДЕЛИЯ, ТО ЭТО НЕОБХОДИМО СДЕЛАТЬ.

В случае, когда за получением изделия с грифом «Коммерческая тайна» прибывает представитель предприятия, куда изделие должно быть отправлено, лицо, выдающее грифованное изделие, должно убедиться в наличии и правильности оформления необходимых документов на получение изделия (доверенность на получение; документ, удостоверяющий личность представителя), а также в наличии охраны для сопровождения груза.

7.4. Проверка наличия (инвентаризация) изделий с грифом «Коммерческая тайна»

Механизм организации и проведения проверки наличия изделий с грифом «Коммерческая тайна» можно принять тот же, что и для проверки наличия грифованных документов, но с некоторыми специфическими особенностями.

В период инвентаризации передача изделий между подразделениями должна быть исключена, поскольку это может негативно повлиять на достоверность результатов изделия, поступающие из внешних организаций, должны приниматься на Центральный склад и там храниться до окончания инвентаризации. Поскольку инвентаризация может быть проведена оперативно (не должна задерживать работу предприятия), то выполнение этих условий не представляется затруднительным.

Инвентаризационными комиссиями в подразделениях должно быть проверено:

1. Наличие грифованных изделий в натуре и соответствие их учетным

данным.

2. Наличие узлов и деталей грифованных изделий, предназначенных для дальнейшей сборки, сведения о которых в бухгалтерию предприятия не представлялись.

3. Режим хранения грифованных изделий.

4. Своевременность и правильность постановки изделия на учет или снятия с учета. Напомним, что изделие с грифом «Коммерческая тайна» снимается с учета как в случае рассекречивания охраняемых сведений, носителем которых оно является, так и в случае «уничтожения» охраняемых сведений (например, полное уничтожение грифованного изделия).

Результаты инвентаризации обязательно направляются также и в бухгалтерию предприятия (для лица, осуществляющего учет изделий с грифом «Коммерческая тайна»).

7.5. Требования к помещениям, предназначенным для разработки, изготовления или хранения изделий с грифом «Коммерческая тайна»

Одним из важных факторов, влияющих на сохранение в тайне охраняемых характеристик изделия, является обеспечение надлежащих условий скрытности в процессе разработки, изготовления или хранения таких изделий. Причем, как правило, наиболее трудно обеспечить защиту охраняемых характеристик изделия на стадии его разработки.

Очень важно на этом этапе своевременно определить, КАКИЕ характеристики разрабатываемого изделия являются коммерческой тайной, КОГДА они могут проявиться и КАКИМ СПОСОБОМ они могут быть установлены лицами, которые не должны, но очень хотят их знать.

В этой связи и должны устанавливаться требования к помещениям, в которых разрабатываются (изготавливаются или хранятся) изделия с грифом «Коммерческая тайна».

ПРИ ЭТОМ ВАЖНО ПОМНИТЬ, ЧТО ВСЯКИЕ ОГРАНИЧИТЕЛЬНЫЕ МЕРЫ ДОЛЖНЫ ВВОДИТЬСЯ ОБОСНОВАННО, А ПРИНЯТИЕ БОЛЬШОГО КОЛИЧЕСТВА ЗАЩИТНЫХ МЕР ЕЛЕ НЕ ОЗНАЧАЕТ, ЧТО ТРЕБУЕМЫЙ РЕЗУЛЬТАТ ПОСЛЕ ИХ ВВЕДЕНИЯ БУДЕТ ДОСТИГНУТ.

Например, гриф «Коммерческая тайна» присвоен изделию в связи с применением особой технологии его изготовления. Причем примененная технология может стать известной только из грифованных документов. В этом случае вряд ли следует принимать другие меры защиты, чем те, которые определены для сохранности материальных ценностей.

Другое дело, если одной из охраняемых характеристик является внешний вид изделия. Тогда необходимо принять меры, чтобы исключить возможность несанкционированного получения изображения изделия или наблюдения за ним.

В некоторых случаях необходимо скрывать характеристики различных излучений, которые могут быть установлены приборами, причем на значитель-

ном расстоянии. Тогда необходимо использовать экранирование помещений или активную радиотехническую маскировку. Приведем некоторые практические рекомендации.

Производственные помещения должны размещаться на охраняемой территории и обеспечиваться сигнализацией.

Окна первого этажа оборудуются решетками и, если это необходимо, матовыми стеклами (зашториваются).

Входные двери обивают железом.

Определен порядок вскрытия и сдачи помещения под охрану.

Входная дверь должна быть постоянно закрытой на замок и оборудована звонковой кнопкой для вызова дежурного по помещению. Дежурный, как правило, назначается из числа сотрудников, постоянно работающих в помещении. Вход в помещение осуществляется по утвержденному списку. Список целесообразно разместить на внутренней стороне входной двери.

Все шкафы и сейфы, используемые для хранения грифованных изделий, в т. ч. и для временного хранения на рабочих местах, должны быть зарегистрирована Передача ключей другому лицу и перемещение сейфов могут производиться только с ведома руководителей подразделений.

По окончании рабочего дня или смены помещения, хранилища и шкафы с находящимися в них грифованными изделиями, запираются и опечатываются уполномоченными или ответственными исполнителями, получившими изделия, и сдаются под охрану.

Уполномоченный в подразделении перед вскрытием обязан проверить целостность оттисков печатей или пломб на дверях, шкафах и сейфах с изделиями. В случае обнаружения повреждения запоров и печатей немедленно ставить в известность руководство подразделения.

ПРИ ЭТОМ САМОСТОЯТЕЛЬНЫХ ДЕЙСТВИЙ ПО ВСКРЫТИЮ НЕ ПРОИЗВОДИТЬ

Перечень таких рекомендаций можно продолжать. Но и из приведенных рекомендаций видно, что они направлены на исключение хищения изделий и несанкционированного доступа к ним.

НАДО ШИРЕ ПРАКТИКОВАТЬ ПОКАЗ ТОГО ФАКТА, ЧТО ИЗДЕЛИЕ ОХРАНЯЮТСЯ (предупредительные надписи, соответствующие хорошо видимые отличительные знаки на дверях помещений.

Что касается возможности получения охраняемой информации при помощи технических средств, то здесь для каждого случая требуется конкретная постановка задачи.

8. ЗАЩИТА ИНФОРМАЦИИ, СОСТАВЛЯЮЩАЯ КОММЕРЧЕСКУЮ ТАЙНУ, ПРИ ОБРАБОТКЕ И ХРАНЕНИИ ЕЕ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

Средства автоматизированной обработки информации с использованием ЭВМ (ПЭВМ) имеют ряд особенностей, позволяющих бесконтрольно манипу-

лировать информацией соответствующих автоматизированных систем (АС) как персоналу АС, так и посторонним лицам, а также скрытно получать доступ к обрабатываемой информации на значительном расстоянии от средств вычислительной техники. Поэтому конфиденциальная информация АС (составляющая коммерческую тайну) без адекватной ее защиты может быть достаточно легко скомпрометирована, вызвав значительные экономические, моральные и другие потери для собственника (владельца) такой информации. В связи с этим, принятие решения о вводе конфиденциальной информации в АС необходимо проводить с учетом определенного риска, который может быть значительно уменьшен или практически исключен с использованием соответствующих средств и мер защиты.

Применительно к АС наиболее опасными действиями по отношению к защищаемой информации являются: утрата информации - неосторожные действия собственника информации, представленной в АС на различных носителях и в файлах, или лица, которому были доверена информация в силу его официальных (производственных) обязанностей в рамках АС, в результате которых информация была потеряна и стала либо могла стать достоянием посторонних лиц;

раскрытие информации - умышленные или неосторожные действия, в результате которых информация, представленная на различных носителях и в файлах, стала доступной для посторонних лиц;

порча информации - умышленные или неосторожные действия, приводящие к полному или частичному уничтожению информации, представленной на различных носителях и в файлах;

кража информации - умышленные действия, направленные на несанкционированное изъятие информации из системы ее обработки, как посредством кражи носителей информации, так и посредством дублирования (копирования) информации, представленной в виде файлов АС;

подделка информации - умышленные или неосторожные действия, в результате которых нарушается целостность (точность, достоверность, полнота) информации, находящейся на различных носителях и в файлах АС;

блокирование информации - умышленные или неосторожные действия, приводящие к недоступности информации в системе ее обработки;

нарушение работы системы обработки информации умышленные или неосторожные действия, приводящие к частичному или полному отказу системы обработки либо создающие благоприятные условия для выполнения вышеперечисленных действий.

Перечисленные действия могут реализовываться в АС посредством следующих атак (каналов, угроз):

1. Незаконное физическое проникновение посторонних лиц в помещения, в которых располагаются средства автоматизированной обработки (хранилища, архивы);

2. Перехват побочных электромагнитных, акустических и других излу-

чений от средств автоматизированной обработки, несущих конфиденциальную информацию, как через традиционный «эфир», так и с использованием наводок таких излучений на вспомогательные технические средства, непосредственно не участвующие в обработке информации (сети питания, телефонные линии, отопление, канализация и т. п.);

3. Использование электроакустического воздействия речи персонала АС на СВТ и вспомогательные технические средства для перехвата речевой информации, содержащей коммерческую тайну, по соответствующему излучению модулированных сигналов от этих средств;

4. Перехват информационных сигналов в линиях и каналах связи средств автоматизированной обработки посредством незаконного к ним подключения;

5. Включение специальных устройств в СВТ, позволяющих несанкционированно получать обрабатываемую в АС информацию, ретранслировать ее с помощью передатчиков, блокировать работу СВТ, уничтожать информацию на различных носителях, уничтожать сами СВТ;

6. Несанкционированное (незаконное) логическое проникновение (вход) в АС посторонних лиц под видом законного пользователя посредством подбора (кражи) пароля или обхода механизма контроля входа в систему (при его наличии);

7. Загрузка посторонней операционной системы (ОС) или программ без средств контроля доступа в ЭВМ АС;

8. Обследование (считывание) освобожденных областей оперативной и внешней памяти, ранее содержавших конфиденциальную информацию и информацию по разграничению доступа (пароли, ключи, коды, матрицы доступа и т. п.), а также отработанных носителей АС (печатных, графических документов);

9. Получение привилегированного статуса для взятия полного контроля над АС посредством изменения системных таблиц ОС и регистров;

10. Изменение установленного статуса объектов защиты АС (кодов защиты, паролей, матрицы доступа);

11. Модификация прикладных и системных программных средств АС с целью обхода (отключения) механизма контроля доступа или выполнения несанкционированных действий в АС;

12. Введение и использование в АС «вредоносных» программных средств для манипулирования или блокирования работы АС.

Сети ЭВМ (ПЭВМ) по сравнению с автономной ЭВМ (ПЭВМ) значительно больше подвержены возможным посягательствам на обрабатываемую в них информацию. Наиболее распространенными угрозами в сети ЭВМ являются: перехват сообщений в каналах передачи; порождение правдоподобных сообщений; маскировка под узаконенный узел сети; подложная идентификация оконечного абонента; несанкционированный доступ со стороны законных абонентов; неправильный выбор маршрута сообщений.

С учетом перечисленных угроз защита конфиденциальной информации в АС строится в виде двух относительно самостоятельных в техническом плане частей, реализующих:

8.1. Основные требования к системам защиты информации

Основными методами защиты информации в АС являются:

физическая охрана средств вычислительной техники (СВТ) (устройств и носителей информации), предусматривающая наличие охраны территории и здания, где размещается АС, с помощью технических средств охраны и/или специального персонала, использование строгого пропускного режима, специальное оборудование помещений АС;

использование средств вычислительной техники (СВТ) в специально защищенном от ПЭМИН и НСД исполнении;

использование сертифицированных средств защиты; проведение специальных исследований и контроль СВТ с целью исключения непредусмотренных включений и добавок;

снижение (исключение) побочных электромагнитных излучений от СВТ;

снижение (исключение) наводок побочных электромагнитных излучений от СВТ на вспомогательные технические средства (ВТС);

снижение (исключение) информативности сигналов побочных электромагнитных излучений и наводок с использованием систем активной защиты (генераторов шума);

идентификация и проверка подлинности (аутентификация) пользователей и других ресурсов АС (программно-аппаратных средств);

персональный допуск пользователей к работе в АС и ее ресурсам, включая взаимодействие с другими ресурсами АС;

надзор за деятельностью пользователей в АС и ее учет, включая средства обеспечения персональной ответственности. пользователей за свои действия в АС;

проверка целостности (отсутствия вредных изменений) ресурсов АС, включая средства защиты информации;

использование криптографических средств защиты информации, находящейся в оперативной и внешней памяти ЭВМ и на различных носителях, а также передаваемой по линиям связи;

применение методов защиты от копирования файлов АС;

периодическое и динамическое тестирование и контроль работоспособности средств защиты, их оперативное восстановление.

Выбор структуры СЗИ и методов защиты осуществляется в процессе создания СЗИ на основании предварительного аналитического и технического обследования АС с учетом государственных нормативных и руководящих документов по защите информации от ПЭМИН и НСД. Требуемое качество СЗИ (надежность защиты информации) задается собственником (владельцем) информации и определяется как на этапе создания, так и эксплуатации СЗИ.

Для выполнения работ по созданию СЗИ могут привлекаться специализированные предприятия, имеющие лицензию на проведение работ по защите коммерческой информации, сертификации средств защиты, аттестации СЗИ АС.

При обработке или хранении в АС информации в рамках СЗИ государственным, коллективные частным и совместным предприятиям, а также частным лицам рекомендуются следующие организационные мероприятия:

выявление конфиденциальной информации и ее документальное оформление в виде перечня сведений, подлежащих защите;

определение порядка установления уровня полномочий субъекта доступа, а также круга лиц, которым это право предоставлено;

установление и оформление правил разграничения доступа, т.е. совокупности правил, регламентирующих права доступа субъектов к объектам;

ознакомление субъекта доступа с перечнем защищаемых сведений и его уровнем полномочий, а также с организационно-распорядительной и рабочей документацией, определяющей требования и порядок обработки конфиденциальной информации;

получение от субъекта доступа расписки о неразглашении доверенной ему конфиденциальной информации;

обеспечение охраны объекта, на котором расположена защищаемая АС (территория, здания, помещения, хранилища информационных носителей) путем установления соответствующих постов, технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими хищение средств вычислительной техники (СВТ), информационных носителей, а также НСД к СВТ и линиям связи АС;

выбор класса защищенности АС в соответствии с особенностями обработки информации (технология обработки, конкретные условия эксплуатации АС) и уровнем ее конфиденциальности;

организация службы безопасности информации (ответственные лица, администратор АС), осуществляющей учет, хранение и выдачу информационных носителей, паролей, ключей, ведение служебной информации СЗИ НСД (генерацию паролей, ключей, сопровождение правил разграничения доступа), приемку включаемых в АС новых программных средств, а также контроль за ходом технологического процесса обработки конфиденциальной информации и т. д.;

разработка СЗИ, включая соответствующую организационно-распорядительную и эксплуатационную документацию;

осуществление приемки СЗИ в составе АС и ее аттестация.

Создание СЗИ рекомендуется проводить по следующим этапам:

1. Проведение аналитического обследования АС с целью оценки возможной уязвимости обрабатываемой в ней коммерческой информации и выработки необходимых требований по ее защите.

На данном этапе, исходя из требований собственника (владельца) ин-

формации и предварительного обследования АС, осуществляется выбор уровня защиты информации - класса защищенности АС от НСД, а также требования по защите информации от ПЭМИН.

2. Проектирование (создание) СЗИ. В процессе создания (разработки) СЗИ на основании установленных требований по защите информации от НСД и ПЭМИН с учетом условий работы АС и заданных собственником (владельцем) информации ограничений на финансовые, материальные, трудовые и другие ресурсы осуществляется выбор или/и разработка конкретных методов и средств защиты. Результатом данного этапа является законченный комплекс аттестованных (сертифицированных) средств и методов защиты информации, имеющий соответствующую необходимую проектную и эксплуатационную документацию.

3. Приемка СЗИ в эксплуатацию. На данном этапе осуществляется внедрение (установка) средств и методов СЗИ в АС, их комплексная проверка и тестирование, необходимое обучение и освоение персоналом АС СЗИ. Устраняются выявленные в процессе .проверки и тестирования недостатки СЗИ. Результатом этого этапа является общая аттестация СЗИ АС.

4. Эксплуатация СЗИ АС. В процессе эксплуатации АС проводится регулярный контроль эффективности СЗИ, при необходимости осуществляется доработка СЗИ в условиях изменения состава программно-аппаратных средств, оперативной обстановки и окружения АС. Контролируются и анализируются все изменения состава АС и СЗИ перед их реализацией отклоняются все модификации АС, снижающие установленную эффективность защиты информации. Периодически (1 раз в год) подтверждается аттестация СЗИ АС.

8.2. Требования к системам защиты информации от несанкционированного доступа

Защита информации от НСД является составной частью общей проблемы обеспечения безопасности информации. Мероприятия по защите информации от НСД должны осуществляться взаимосвязано с мероприятиями по специальной защите основных и вспомогательных средств вычислительной техники от ПЭМИН.

Комплекс программно-аппаратных средств и организационных (процедурных) решений по защите информации от НСД реализуется в рамках системы защиты информации от НСД (СЗИ НСД), состоящей условно из следующих четырех подсистем: управления доступом; регистрации и учета; криптографической; обеспечения целостности.

Собственником (владельцем) конфиденциальной информации АС при участии экспертной комиссии и заинтересованных лиц выбирается приемлемый класс защищенности АС от НСД (при необходимости с привлечением специалистов по защите информации), исходя из условий и режима работы АС и требуемой надежности защиты информации. Выбранная классификация защищенности АС оформляется актом и утверждается собственником (владельцем) кон-

фиденциальной информации АС.

К числу определяющих признаков, по которым производится группировка АС в различные классы, относятся:

наличие в АС информации различного уровня конфиденциальности; уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации;

режим обработки данных в АС: коллективный или индивидуальный.

Конкретный состав СЗИ НСД определяется, исходя из выбранного для данной АС класса защищенности в соответствии с документом «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».

В зависимости от условий конкретной АС, определяемых, главным образов установленным классом защищенности АС в рамках подсистем управления доступом, регистрации и учета, обеспечения целостности и криптографической подсистемы рекомендуется реализовать (выполнить) следующие функции - требования по соответствующим классам.

Подсистема управления доступом должна включать средства идентификации, проверки подлинности (аутентификации) и контроль доступа пользователей и их программ к следующим ресурсам:

к системе;

к терминалам;

к ЭВМ (ПЭВМ), узлам сети ЭВМ (ПЭВМ);

к каналам связи;

к внешним устройствам ЭВМ (ПЭВМ);

к программа к томам, каталогам, файлам, записям, полям записей.

Элементы идентификации, проверки подлинности и контроля доступа к ресурсам реализуются при наличии в АС указанных ресурсов и в случае отсутствия полномочий на доступ к ним у некоторых пользователей. Контроль доступа субъектов к защищаемым ресурсам осуществляется в соответствии с матрицей доступа.

Помимо средств контроля доступа данная подсистема при наличии нескольких уровней конфиденциальности информации должна включать средства управления потоками информации, т. е. контроля передачи информации между строго установленными ресурсами (носителями) с учетом наличия разрешения на такой вид обмена. Управление потоками информации осуществляется с помощью меток конфиденциальности. При этом уровень конфиденциальности защищаемых объектов (накопителей) должен быть не ниже уровня конфиденциальности записываемой на них информации.

Подсистема регистрации и учета должна включать средства регистрации и учета следующих событий и/или ресурсов:

входа/выхода пользователей в/из системы (узла сети);

выдачи печатных (графических выходных документов;

запуска/завершения программ и процессов (заданий, задач), использующих защищаемые файлы;

доступа программ пользователей к защищаемым файлам включая их создание и удаление, передачу по линиям и каналам связи;

доступа программ пользователей к терминалам, ЭВМ, узлам сети ЭВМ, каналам и линиям связи, внешним устройствам ЭВМ, программам, томам, каталогам; изменения полномочий субъектов доступа; создаваемых защищаемых объектов доступа; учета носителей информации. Кроме этого, данная подсистема должна включать средства очистки (обнуления, обезличивания) областей оперативной памяти ЭВМ и внешних накопителей, использованных для обработки и/или хранения защищаемой информации.

Криптографическая подсистема должна предусматривать шифрование конфиденциальной информации, записываемой на совместно используемые различными субъектами доступа (разделяемые) носители данных, а также на съемные носители данных (ленты, диски, дискеты, микрокассеты и т.п.) долговременной внешней памяти для хранения за пределами сеансов работы санкционированных субъектов доступа. Доступ к операциям шифрования и/или криптографическим ключам должен контролироваться посредством подсистемы управления доступом. При этом должны использоваться сертифицированные средства криптографической защиты. Их сертификация проводится специальными сертификационными центрами или специализированными предприятиями, имеющими лицензию на проведение сертификации криптографических средств защиты.

Уровень реализации функций СЗИ НСД должен обеспечивать ее целостность для всех режимов работы АС.

Подсистема обеспечения целостности СЗИ НСД является обязательной для любой СЗИ и включает организационный, программно-аппаратные и другие средства и методы, обеспечивающие:

физическую охрану СВТ (устройств и носителей информации), территории и здания, где размещается ЛС, с помощью технических средств охраны и специального персонала, строгий пропускной режим, специальное оборудование помещений АС;

недоступность средств управления доступом, учета и контроля со стороны пользователей с целью их модификации, блокирования или отключения;

контроль целостности программных средств АС и СЗИ на предмет их несанкционированного изменения;

периодическое и/или динамическое тестирование функций СЗИ НСД с помощью специальных программных средств;

наличие администратора (службы) защиты информации, ответственного за ведение, нормальное функционирование и контроль работы СЗИ НСД;

восстановление СЗИ НСД при отказе и сбое;

применение сертифицированных (аттестованных) средств и методов защиты, сертификация которых проводится специальными сертификационными

центрами или специализированными предприятиями, имеющими лицензию на проведение сертификации средств защиты СЗИ НСД, для низких классов защищенности допускается проведение сертификации самим предприятием (собственником).

Контроль программной среды общесистемных средств и СЗИ НСД, принятой в эксплуатацию, должен быть обеспечен для каждой АС, обрабатывающей конфиденциальную информацию. Целостность программной среды обеспечивается качеством приемки программных средств АС, предназначенных для обработки конфиденциальной информации.

Практическое создание средств защиты информации, удовлетворяющих перечисленным требованиям, осуществляется в рамках аппаратных средств и управляющих программ операционных систем ЭВМ (ПЭВМ), а также в рамках программных средств, расширяющих возможности операционных систем в случае их применения.

8.3. Требования к системам защиты информации от перехвата электромагнитных излучений и наводок (ПЭМИН)

В практике защиты конфиденциальной информации АС от перехвата за счет ПЭМИН применяются следующие методы защиты:

1. Применение средств вычислительной техники в защищенном от ПЭМИН исполнении.

2. Реализация объектовых мер и средств защиты.

3. Использование специальных организационных мероприятий по защите информации от ПЭМИН.

4. Использование технических средств защиты. Наибольшая эффективность защиты от ПЭМИН достигается комплексным сочетанием перечисленных методов в рамках системы защиты информации от ПЭМИН. Выбор методов защиты коммерческой информации в АС от ПЭМИН необходимо проводить с учетом их технико-экономической целесообразности и анализа конкретных условий АС. Разработку системы защиты информации от ПЭМИН в АС должны проводить соответствующие специалисты или специализированные предприятия, имеющие лицензию на данный вид деятельности.

Возможность применения СВТ в защищенном исполнении рассматривается на начальных этапах создания СЗИ. При положительном решении оформляется соответствующий заказ на приобретение таких СВТ у их производителя. При отсутствии требуемых отечественных СВТ в защищенном исполнении следует ориентироваться на СВТ зарубежного производства, выпускаемых с учетом технологии TEMPE5T. СВТ зарубежного производства, предназначенные для обработки конфиденциальной информации, следует использовать в АС после проведения специальных проверок на предмет отсутствия в них непредусмотренных включений и добавок. Такие проверки проводят специализированные предприятия, имеющие соответствующую лицензию.

В случае отсутствия СВТ в защищенном исполнении в АС или недоста-

точности их характеристик по защищенности на основании аналитического обследования АС рассматривается применение объектовых, мер по защите от ПЭМИН. Такие меры могут предусматривать:

создание контролируемой зоны СВТ (территории) в пределах которой исключается или значительно затрудняется перехват сигналов ПЭМИН;

создание специальной зоны, в пределах которой запрещается размещение вспомогательных технических средств (ВТС), исключаются или значительно снижаются наводки на эти средства, исключается (затрудняется) посторонее к ним подключение. ВТС (телефонные средства и системы, цепи освещения, трубопроводы и металлоконструкции, средства и системы кондиционирования, средства охраны и сигнализации и т.п.), имеющие выход за пределы контролируемой зоны, необходимо удалять от основных технических средств;

организацию питания и заземления СВТ, дооборудование помещений, специальное размещение и монтаж СВТ и ВТС, снижающие ПЭМИН.

При недостаточности объектовых мер рекомендуется предусматривать меры организационного характера, включающие организацию охраны и контроля доступа к зонам размещения СВТ и ВТС, проверку цепей и коммуникаций на предмет отсутствия непредусмотренных отводок и подключений и т. п.

Наиболее распространенной системой технической защиты от ПЭМИН является система, которая использует активный метод зашумлению побочных электромагнитных излучений от электронной вычислительной техники (ЭВТ) и наводок в процессе обработки защищаемой информации. Для такой защиты используются специально разработанные генераторы шума с использованием специальной системы антенн. Генераторы устанавливаются в помещениях, где обрабатывается защищаемая информация и включается до начала обработки информации на ЗВТ. Для исключения информативности наводок на ВТС к последним подключается антенная система генераторов шума.

Создание системы активной защиты (САЗ) проводится с использованием специальных изделий и устройств, примером которых являются САЗ «Волна-3М» и «Вектор-4». Требования и рекомендации по изделиям «Волна-3М» и «Вектор-4» содержатся в их проектной документации (издание СНПО «ЭЛЕРОН») и в отраслевых материалах ОРТМ ЭВТ-81.

В рамках технической защиты могут использоваться дополнительные конструктивные решения СВТ, снижающие ПЭМИ.

Для защиты линий связи СВТ от ПЭМИН и подключений наиболее эффективными являются волоконно-оптические системы связи и криптографические средства.

Эффективность защиты от ПЭМИН после внедрения всех мероприятий исследуется по специальной методике.

Более детальные рекомендации и требования по защите разрабатываются с учетом государственных нормативных документов по защите коммерческой информации от ПЭМИН.

9. ПРИЛОЖЕНИЯ

Приложение 1

Наименование предприятия

А К Т

_____ № _____

О недостаче документов

Мы, _____
(должности, Ф. И. 0. , сотрудника, получившего
_____
пакет и руководителя подразделения по ведению делопроизводства
_____
документов с грифом «Коммерческая тайна»)
составили настоящий акт в том, что при получении пакета №_____ (Документа №_____), доставленного из
_____
_
(наименование предприятия)
обнаружено _____
_____
_____
_____

Должность, подпись, инициалы, фамилия.

Должность, подпись, инициалы, фамилия.

Приложение 2

Карточка учета входящих документов
с грифом «Коммерческая тайна»

Лицевая сторона

1. Дата регистрации	2. Входящий номер	3. Исходящий номер и дата поступившего документа	Количество листов	
			4. Основного	5. Приложения
6. Наименование отправителя				
7. Краткое содержание				
8. Подшивка документа		9. Регистрация приложения		
номер дела	подпись и дата	вид	инв. номер	подпись дата

Оборотная сторона

10. Дата выдачи	Кол-во листов		13. Кому выдан или куда отправлен	14. Роспись в получении номер сопроводительного документа об отправке (реестр)	15. Дата возвр. и подпись
	11. Осн.	12. Прилож.			
16. Для разных отметок:					

Приложение 3

Карточка учета подготовленных документов с грифом «Коммерческая тайна»

1. Дата регистрации	2. Номер документа	4. Количество	
		экземпляров	листов в экземпляре

5. Содержание

Движение документа				
6. Дата	7. Количество экз. листов	8. Кому выдан или куда отправлен	9. Роспись в получении или номер сопровод. документа при отправке	10. Дата возврата и подпись
II. Приложение к исходящему				

Оборотная сторона:

Отметка об уничтожении документа и черновика	
12. №_____ в_____экз. на_____листах уничтожен. Акт №_____от_____ Подпись_____	13. Черновик на_____ лист. Уничтожен “ ____” _____2000г Подпись_____
14. Для разных отметок:	

Приложение 4

Карточка инвентарного учета документов с грифом «Коммерческая тайна»

Лицевая сторона

1. Инв.№	2._____ (наименование документа)				
3. Дата	4. Уч. номер, вошедшие в документ	5. Откуда поступил или кем разработан	6. № экз.	7. Кол-во листов в экз.	8. Отметка об отправке или уничтожении (номер сопроводительного письма, реестра, акта, описи), снятия с учета, подпись дата.
9. Номер наряда, по которому размножен документ					

Оборотная сторона:

3	4	5	6	7	8

Приложение 5

Карточка учета выдачи документов с грифом «Коммерческая тайна«

Документ (Дело) №_____

_____

Наименование документа (Дела)

Дата выдачи	Кол-во Листов	Фамилия исполнителя	Роспись за получение	Дата возврата	Подпись о прием.

Приложение 6

РАСПИСКА

Дана тов. _____
в том, что мною, _____
получены на временное пользование документы за №№ _____
_____

Всего на _____листах.
«____» _____ 2000 г.

_____
(Подпись)

ЛИТЕРАТУРА

1. Алексенцев А.И. Классификация и систематизация исполненных конфиденциальных документов: Учеб. пособие. М., 1989.
2. Алексенцев А.И. Подготовка и издание конфиденциальных документов: Учеб. пособие. М., 1990.
3. Илюшенко М.П. Организация документооборота: Учеб. пособие. М.: МГИАИ, 1984.
4. Информационно-коммерческая безопасность: Защита коммерческой тайны: Пособие. Спб., 1993.
5. Коммерческая тайна предприятия. М.: ОКБ «Прогресс», 1993.
6. Кузнецова Т.В., Степанов Е.А, Филиппов Н.Г. Делопроизводство и техническая документация: Учеб. М.: Высш. шк., 1991.
7. Левин А.В. Секрет фирмы. М.: Машиностроение, 1992.
8. Ярочкин В.И., Халяпин Д.Б. Основы защиты информации. Служба безопасности предприятия: Учеб. пособие. М., 1993.
9. Все о защите коммерческой информации. М.: Махаон, 1992.
10. Герасименко А,В., Гришаев С./7., Павлов Д.В. и др. Основы защиты коммерческой информации и интеллектуальной собственности. М.: Науч.-информ. внедрен, фирма «ЮНИС», 1991.
11. Костомаров М.Н., Соколов А.В., Степанов Е.А. Информационное обеспечение управления: Учеб. пособие.: МГИАИ, 1990.
12. Практика защиты коммерческой тайны в США: Руководство по защите деловой информации. М.: СП «Крокус-Инернациональ», 1990.
13. Руководство по организации защиты коммерческой тайны. Ч. 1—3. М.: Минавтопром СССР, 1991.
14. Сверчков Л.М, Чурляев Ю.А Защита коммерческой тайны в производственно-предпринимательской деятельности предприятия. М.: ЦИПК АП, 1991.
15. Ярочкин В.И. Предприниматель и безопасность: В 2 ч. М., 1994.
16. Ярочкин В,И, Служба безопасности коммерческого предприятия. М.: «Ось-89». 1995.

СОДЕРЖАНИЕ

Макаревич Олег Борисович
Бабенко Людмила Константиновна
Шилов Александр Кимович
Коваленко Александр Валентинович

Методическое пособие
Основы защищенного делопроизводства
по курсу
Технология защищенного документооборота
Часть 2
Для студентов специальностей 075300, 075400, 075500

Ответственный за выпуск Коваленко А.В.
Редактор Монахова Е.Л.
Корректор Пономарева Н.В.

ЛР № 020565 Подписано к печати
Формат 60x84 1/16. Бумага офсетная
Печать Офсетная Усл. п. л.- 5.0 Уч.- изд. л.- 4.7
Заказ № Тираж 100 экз.
«С»

Издательство Таганрогского государственного радиотехнического университета
ГСП 17 А, Таганрог, 28, Некрасовский, 44
Типография Таганрогского государственного радиотехнического университета
ГСП 17 А, Таганрог, 28, Энгельса, 1